MasterCard International

MasterCard® PayPass™

M/Chip, Issuer Implementation Requirements

v.1-A4 6/06

TABLE OF CONTENTS

1 USING THESE REQUIREMENTS 4
1.1 Purpose 4
1.2 Scope 4
1.3 Audience 4
1.4 Overview 5
1.5 Language Use 5
1.6 Related Publications 6
1.7 Related Information 7
1.8 Abbreviations 8
1.9 Notations 9
1.10 Further Information 10

2 INTRODUCTION 11
2.1 What Is MasterCard *PayPass*? 11
2.2 *PayPass* Product Overview 11
2.3 Contactless Technology 12
2.4 Processing *PayPass* Transactions 13
2.5 Proprietary Contactless Products 13

3 ISSUER IMPACT 14
3.1 Introduction 14
3.2 *PayPass* Program Enrollment 14
3.3 Card Design 15
3.3.1 Antenna 15
3.3.2 *PayPass* Logo and Design Approval 16
3.3.3 Non-Card Form Factors 16
3.4 Ordering Cards 16
3.5 *PayPass*—M/Chip Card Application 17
3.5.1 *PayPass*—M/Chip Data Objects 18
3.5.2 *PayPass*—M/Chip Application Behavior 18
3.6 Multiapplication 21
3.7 Personalization 22
3.8 Card Delivery 22
3.9 Issuer Host System—Authorization 23
3.9.1 Identifying the *PayPass* Profile 23
3.9.2 Authorizing *PayPass*—Mag Stripe Transactions 23
3.9.3 Authorizing *PayPass*—M/Chip Transactions 24
3.10 Issuer Host System—Clearing 25
3.10.1 Identifying the *PayPass* Profile 25
3.10.2 Clearing *PayPass*—Mag Stripe Transactions 26
3.10.3 Clearing *PayPass*—M/Chip Transactions 26
3.11 Issuer Testing 26
3.11.1 Card Validation 26
3.11.2 Network Interface Validation 27
3.11.3 End-to-End Demonstration (ETED) 27
3.12 Staff Training 27

4 PERSONALIZATION OF THE *PAYPASS*—M/CHIP APPLICATION 28
4.1 Introduction 28
4.2 File Organization and AFL 28
4.3 Configuring the AIP (*PayPass*) 33
4.4 Configuring the Application Control (*PayPass*) 34
4.4.1 Mag Stripe Grade Issuer Activated 36
4.4.2 Card Issuer Action Code (CIAC)—Default on CAT3 36
4.4.3 Key for Offline Encrypted PIN Verification 36
4.4.4 Offline Encrypted PIN Verification 36
4.4.5 Offline Plain Text PIN Verification 36
4.4.6 Static CVC3 36
4.4.7 Include *ATC* 36
4.5 Configuring the CIACs (*PayPass*) 37
4.6 Configuring Card Risk Management Data Objects 37
4.7 *PayPass*—Mag Stripe Data Objects 37
4.7.1 *Bitmaps* 38
4.7.2 *Track 2 Data* 40
4.7.3 *Track 1 Data* 41
4.7.4 *IVCVC3$_{TRACK1}$ and IVCVC3$_{TRACK2}$* 42
4.7.5 *Static CVC3$_{TRACK1}$ and Static CVC3$_{TRACK2}$* 42
4.7.6 *Mag Stripe CVM List* 43
4.7.7 *Mag Stripe Application Version Number (Card)* 43

APPENDICES 44
Appendix A, *PayPass* Network Upgrade 44
Appendix B, Data Objects Personalization Values 46
Appendix C, Glossary 62

Copyright

The information contained in this manual is proprietary and confidential to MasterCard International Incorporated (MasterCard) and its members.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of MasterCard.

Media

This document is available in both electronic and printed format.

MasterCard International—CCOE
Chaussée de Tervuren, 198A
B-1410 Waterloo
Belgium

E-mail: specifications@paypass.com

1. USING THESE REQUIREMENTS

1.1 Purpose

This document provides guidelines for issuers that want to deploy MasterCard® *PayPass*™—M/Chip.

The document is written for issuers that have already deployed M/Chip 4 (contact) cards.

1.2 Scope

This document summarizes *PayPass* to enable issuers to easily understand the requirements for issuing *PayPass* products. More information on MasterCard *PayPass* products can be found in the *MasterCard PayPass Product Guide*.

1.3 Audience

This document is intended for use by issuers that want to deploy the MasterCard *PayPass* product on a card. The target audience includes:

- Staff working on implementation projects.
- Operations staff who need to understand the impact of *PayPass*—M/Chip on their activities.
- Staff from related business functions affected by *PayPass* (for example, product managers, risk managers).

It is assumed that the audience is already familiar with chip deployment in general and M/Chip 4 in particular. It is also assumed that the audience has a basic understanding of ISO/IEC 14443 contactless technology.

1.4 Overview

The following table provides an overview of the chapters in this manual:

CHAPTER	DESCRIPTION
Table of Contents	A list of the manual's tabbed sections and subsections. Each entry references a section and page number.
1. Using These Requirements	Describes the purpose and contents of the manual.
2. Introduction	Provides an introduction to the MasterCard *PayPass* product. Gives a high-level description of both the *PayPass*—M/Chip and *PayPass*—Mag Stripe products.
3. Issuer Impact	Analyzes the impact for a card issuer upgrading an existing M/Chip 4 contact-only infrastructure with the *PayPass* product.
4. Personalization of the *PayPass*—M/Chip Application	Describes the technical details for the personalization of the *PayPass*—M/Chip application.
Appendix A *PayPass* Network Upgrade	Describes the network updates required to support *PayPass*.
Appendix B Data Objects Personalization Values	Describes all the *PayPass*—M/Chip data objects that require personalization and provides an example for each of the data objects.
Appendix C Glossary	Glossary of terms used in this document.

1.5 Language Use

The spelling of English words in this manual follows the convention used for U.S. English as defined in *Webster's New Collegiate Dictionary*. An exception to the above spelling rule concerns the spelling of proper nouns. In this case, we use the local English spelling.

1.6 Related Publications

The following publications contain material directly related to the contents of these requirements:

1.	*Card Quality Management—Infrastructure Quality Requirements*
2.	*Compliance Assessment and Security Testing Program*
3.	*M/Chip 4 Card Application Specifications for Credit and Debit*
4.	*M/Chip 4 Security & Key Management*
5.	*Addendum to M/Chip 4 Card Application Specifications*,
6.	*M/Chip Functional Architecture for Debit and Credit*
7.	*M/Chip 4 Issuer Guide for and Debit Credit Parameter Management*
8.	*MasterCard PayPass Product Guide*
9.	*PayPass—Mag Stripe Technical Specification*
10.	*PayPass—M/Chip Technical Specification*
11.	*PayPass—ISO/IEC 14443 Implementation Specification*
12.	*PayPass—Mag Stripe Security Architecture*
13.	*PayPass—M/Chip Security Architecture*
14.	*PayPass—M/Chip Vendor Testing Guide*
15.	*Card Design Standards Manual*
16.	*Card Personalization Validation Guide*
17.	*PayPass Branding Guidelines*
18.	*Security Rules and Procedures*
19.	*Protecting MasterCard PayPass Cards and Devices in the Mail*

1.7 Related Information

The following reference materials may be of use to the reader of this manual:

ISO 639:1988	Codes for the representation of names and languages.
ISO/IEC 7811/2	Identification cards—Recording technique—Part 2: Magnetic stripe.
ISO/IEC 7813	Identification cards—Financial transaction cards.
ISO/IEC 7816-4	Information technology—Identification cards—Integrated circuit(s) cards with contacts—Part 4: Inter-industry commands for interchange.
ISO/IEC 10116	Information Technology—Modes of operation of an n-bit block cipher algorithm.
ISO/IEC 14443-1	Identification cards—Contactless integrated circuit(s) cards—Proximity cards—Part 1: Physical characteristics.
ISO/IEC 14443-2	Identification cards—Contactless integrated circuit(s) cards—Proximity cards—Part 2: Radio frequency power and signal interface.
ISO/IEC 14443-3	Identification cards—Contactless integrated circuit(s) cards—Proximity cards—Part 3: Initialization and anti-collision.
ISO/IEC 14443-4	Identification cards—Contactless integrated circuit(s) cards—Proximity cards—Part 4: Transmission protocol.
ISO/IEC 15693	Specification for Contactless Integrated Vicinity Cards. The ISO 15693 specification is broken into three main sections: (1) describes the "Physical Characteristics," (2) describes the "Signal Interface," and (3) describes the "Transmission Protocol."
EMV BOOK 1	Integrated Circuit Card Specification for Payment Systems: Application Independent ICC to Terminal Interface Requirements. Version 4.1, May 2004.
EMV BOOK 2	Integrated Circuit Card Specification for Payment Systems: Security & Key Management. Version 4.1, May 2004.
EMV BOOK 3	Integrated Circuit Card Specification for Payment Systems: Application Specification. Version 4.1, May 2004.
EMV BOOK 4	Integrated Circuit Card Specification for Payment Systems: Cardholder, Attendant and Acquirer Interface Requirements. Version 4.1, May 2004.

1.8 Abbreviations

The following abbreviations are used in these requirements:

ABBREVIATION	DESCRIPTION
AFL	Application File Locator
AID	Application Identifier
AIP	Application Interchange Profile
an	Alphanumeric
ans	Alphanumeric Special
APDU	Application Protocol Data Unit
API	Application Priority Indicator
ARQC	Authorization Request Cryptogram
ASCII	American Standard Code for Information Interchange
ATC	Application Transaction Counter
b	Binary
CA	Certification Authority
CAST	Compliance Assessment Security Testing
CAT	Cardholder Activated Terminal
CDA	Combined Data Authentication
CDOL	Card Data Object List
CIAC	Card Issuer Application Code
CRM	Card Risk Management
CSK	Common Session Key
CVC	Card Verification Code
CVM	Cardholder Verification Method
CQM	Card Quality Management
DDA	Dynamic Data Authentication
DDOL	Dynamic Data Object List
EMV	Europay MasterCard Visa
ETED	End-to-end demonstration
FeliCa™	Contactless IC card technology developed by Sony
FCI	File Control Information
hex	Hexadecimal
IAC	Issuer Action Code
ICC	Integrated Circuit Card
HIS	Issuer Host System
ISO	International Organization for Standardization

ABBREVIATION	DESCRIPTION
MAC	Message Authentication Code
MIFARE™	Contactless IC card technology developed by Philips
LRC	Longitudinal Redundancy Check
Nn	Numeric
PAN	Primary Account Number
PIN	Personal Identification Number
POS	Point of Sale
PPSE	*PayPass* Payment System Environment
PSE	Payment System Environment
RSA	Rivest, Shamir and Adleman
RFU	Reserved for Future Use
SDA	Signed Static Data Authentication
SFISFI	Short File Identifier
SSAD	Signed Static Application Data
TC	Transaction Certificate
TVR	Terminal Verification Results
UDOL	Unpredictable Data Object List
UN	Unpredictable Number

1.9 Notations

NOTATION	DESCRIPTION
'0' to '9' and 'A' to 'F'	16 hexadecimal digits. Values expressed in hexadecimal form are enclosed in single quotes (i.e., '_'). For example, 27509 decimal is expressed in hexadecimal as '6B75')
1001b	Binary notation. Values expressed in binary form are followed by a lowercase b.
"abcd"	an or ans string
#	Number
[…]	Optional part
xx	Any value
Data Object	Data objects are written in *italics* to distinguish them from the text.
COMMAND APDU	Command APDUs are written in CAPITALS to distinguish them from the text.

1.10 Further Information

Further information on the above and the overall *PayPass* program are available in the *MasterCard PayPass Product Guide* and the *PayPass Technical Specifications*. Questions may also be addressed to the following e-mail addresses:

General: paypass@mastercard.com

Specifications: specifications@paypass.com

Testing/approval: testing@paypass.com

Chip Technical Help: chip_help@mastercard.com

2. INTRODUCTION

2.1 What Is MasterCard *PayPass*?

MasterCard *PayPass* is a "proximity payment" program for consumers to pay at the point of sale using contactless technology. To pay, the consumer taps their *PayPass* card on the *PayPass* reader. There is no need for the consumer to insert, swipe, or hand over the *PayPass* card. *PayPass* is targeted at speed and convenience, e.g., payment at fuel pumps, vending machines, and toll booths.

The generic term "proximity payment" is used when the payment mechanism is up to 10 meters from the point of sale. While the proximity program covers multiple technologies and ranges, this document deals only with the MasterCard *PayPass* program built on the *PayPass*—ISO/IEC 14443 implementation technology up to a range of 10 cm (4 inches).

2.2 *PayPass* Product Overview

This section gives a brief introduction to the two products that are part of the *PayPass* program: *PayPass*—Mag Stripe and *PayPass*—M/Chip.

PayPass—Mag Stripe is developed to allow *PayPass* payments using authorization networks that presently support magnetic-stripe authorization for credit or debit applications. A *PayPass*—Mag Stripe card stores *Track 1* and *Track 2 Data* with a discretionary data field that contains a new Card Verification Code (known as CVC3).

PayPass—M/Chip is developed to allow *PayPass* payments in a market that is oriented toward offline acceptance. To manage the offline risk, card and terminal perform offline risk management and offline card authentication (e.g., static data authentication). A *PayPass*—M/Chip card and terminal are capable of accepting or rejecting transactions offline.

Interoperability is a major *PayPass* requirement. A *PayPass*—Mag Stripe card can be used at both *PayPass*—Mag Stripe terminals and *PayPass*—M/Chip terminals. The terminal will always format the transaction data in the same way as a magnetic stripe transaction. Cardholders can use *PayPass*—M/Chip cards at both *PayPass*—Mag Stripe terminals and *PayPass*—M/Chip terminals. When used at a *PayPass*—M/Chip terminal, transactions are formatted in the same way as M/Chip transactions. When used at a *PayPass*—Mag Stripe terminal, transactions are formatted in the same way as *PayPass*—Mag Stripe transactions.

This document is written with the assumption that issuers already have the infrastructure in place for issuing and managing (contact) M/Chip 4 cards.

2.3 Contactless Technology

The *PayPass*—M/Chip application is designed to extend the M/Chip 4 application with a contactless interface. Hence, *PayPass*—M/Chip products are implemented on a dual interface card (i.e., a card with an ISO/IEC 7816-4 contact interface and an ISO/IEC 14443 contactless interface).

To exchange data over the contactless interface, both the card and the terminal need to be equipped with an antenna as illustrated in Figure 1.

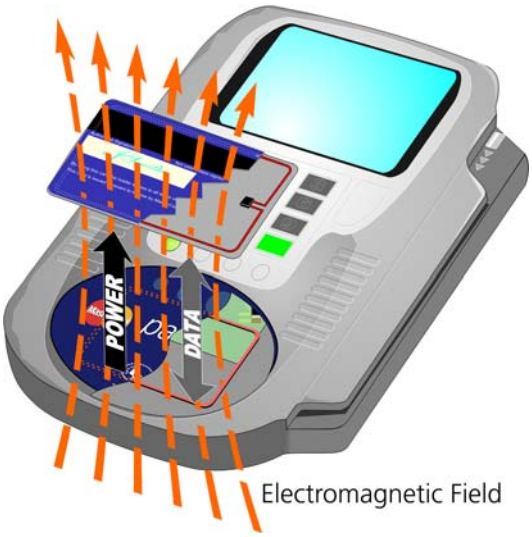


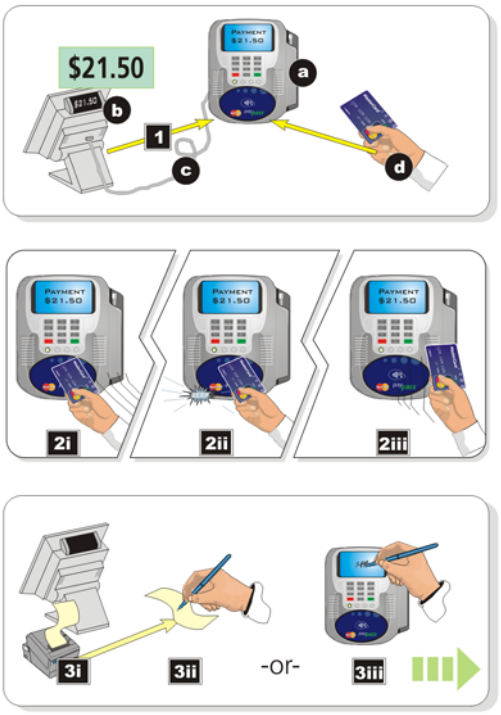
Figure 1, Reader and Card Configuration

The basic components required for a *PayPass* contactless transaction are a contactless reader (in the terminal) and a transponder (in the card). The contactless reader consists of an antenna connected to an electronic circuit. The transponder consists of an antenna connected to an integrated circuit. The reader-transponder combination behaves like a transformer.

An alternating current is passed through the reader's antenna to create an electromagnetic field, which induces a current in the transponder's (card's) antenna. The transponder converts the electromagnetic field transmitted by the contactless reader into a DC voltage. This DC voltage powers up the card's integrated circuit. The specific case where the transponder is a contactless card is shown in Figure 1.

2.4 Processing *PayPass* Transactions

A typical *PayPass*—M/Chip transaction is shown in Figure 2.



Transaction amount sent to *PayPass*—M/Chip terminal (a) from the electronic cash register (b). The *PayPass*—M/Chip terminal (a) is connected to the electronic cash register via a cable (c) so the amount is only entered once.

(2i) Cardholder presents *PayPass* card to *PayPass*—M/Chip terminal.

(2ii) *PayPass*—M/Chip terminal reads data from PayPass card.

(2iii) *PayPass* card is removed.

If required, a receipt is printed (3i) and a cardholder signature is physically (3ii) or electronically (3iii) captured.

Figure 2, Processing *PayPass*—M/Chip Transactions

Network messages for *PayPass* transactions include specific values in existing subelements to indicate the magnetic stripe equivalent data or the M/Chip data was supplied by a contactless chip. Appendix A of this document carries full details of these field settings.

2.5 Proprietary Contactless Products

A number of markets (e.g., public transport, parking garages, toll roads, and fuel dispensers) have already adopted some form of wireless technology for payment transactions. *PayPass* allows issuers to access these markets.

The *PayPass* technology is flexible enough to coexist with proprietary schemes, as indicated in the following examples:

- The card and/or terminal may support both *PayPass* and *FeliCa*. When used in the domestic environment, the card will use *FeliCa* technology. When used abroad, the card will use the *PayPass* technology on international terminals.
- The card and/or terminal can support proprietary technology based on memory cards (e.g., MIFARE emulation). With the appropriate configuration, *PayPass* cards and terminals can support proprietary loyalty applications and ticketing applications.
- The card and/or terminal may support a totally different standard (e.g., ISO 15693) in addition to *PayPass*.

3. ISSUER IMPACT

3.1 Introduction

This section analyzes what a card issuer must do to upgrade an existing M/Chip 4 contact-only infrastructure to include the *PayPass* product. This section is organized in a chronological way to give the new *PayPass* issuer an understanding of the stages required and the order in which they must be done.

As the *PayPass*—M/Chip application also supports the *PayPass*—Mag Stripe application, this section also covers *PayPass*—Mag Stripe processing.

3.2 *PayPass* Program Enrollment

Issuers wishing to participate in the MasterCard *PayPass* Program must complete the *PayPass* Program Enrollment Form.

When the enrollment form has been processed, issuers will receive the guides associated with the program. The *PayPass* Program Enrollment Form is requested by sending an e-mail to specifications@paypass.com.

Once enrolled, issuers will receive the following technical documents:

- *PayPass Product Guide,* containing the *PayPass* product description
- *PayPass ISO/IEC 14443 Implementation Specifications,* containing *PayPass* transport layer requirements
- *PayPass—Mag Stripe Technical Specification* containing the *PayPass*—Mag Stripe application information
- *PayPass—M/Chip Technical Specification,* containing the contactless extension to the M/Chip 4 contact application
- *PayPass Branding Standards*, providing an understanding of how to use the MasterCard *PayPass* identifier
- *PayPass—Mag Stripe Security Architecture,* containing an analysis of *PayPass*—Mag Stripe application security
- *PayPass—M/Chip Security Architecture,* containing an analysis of *PayPass*—M/Chip application security

3.3 Card Design

Issuers wishing to issue *PayPass* cards must obtain approval from MasterCard Card Design Management (CDM) for their card design.

Figure 3 shows that *PayPass*—M/Chip cards have two specific features (the embedded antenna and the *PayPass* identifier) that differ from regular M/Chip 4 (contact only) cards. Issuers must ensure they can meet requirements for these features.

Figure 3, Card Schematics

3.3.1 Antenna

As the name suggests, contactless smart cards need not come into contact with the card reader. The card contains a coil or antenna to realize the contactless read/write operation.

The position of the antenna in the card imposes embossing restrictions. Issuers should be aware of this and ensure both embossing and antenna requirements are met with a specific card design.

Depending on the inlay technology used, it may not be possible to have a fourth line of embossing. The issuer should not automatically assume that the fourth line of embossing is possible on *PayPass* cards. When a fourth line of embossing is required, the issuer should clearly communicate this to the card manufacturer so that an inlay/antenna configuration can be chosen that allows for it.

It must be noted that the adapted antenna configuration may lead to a reduced read range due to its smaller size.

NOTE

MasterCard can supply a list of card manufacturers that support the fourth line of embossing. Please contact MasterCard on paypass@mastercard.com for this information.

3.3.2 *PayPass* Logo and Design Approval

When a card is *PayPass* enabled, the *PayPass* logo must be printed on the card. Before issuing *PayPass* cards, the issuer must submit the card design to MasterCard for approval, even if a similar design has already been approved.

Submitting a card design for approval is done by sending the design to testing@paypass.com, stating clearly that the card will be *PayPass* enabled.

3.3.3 Non-Card Form Factors

To date, unlike *PayPass*—Mag Stripe, the *PayPass*—M/Chip application cannot be used on non-card form factors. The *PayPass*—M/Chip application has been developed around the idea of dual-interface cards.

With contact chip cards, the issuer is informed during online transactions about previous transactions and, importantly, the issuer is able to return an instruction to the card using a script command. The instruction contained in the script could be used to block the application or reset the offline counters in the card (so that the card is "renewed" for offline transactions).

With contactless transactions, these messages cannot be delivered to the card (or cardholder device). A typical contactless transaction time is 0.5 seconds or less. There is no way that an issuer response to an authorization request can reach the terminal and card in that time. This is the reason the *PayPass*—M/Chip application has been developed around the idea of dual-interface cards. The risk parameters in the card are reset during online contact transactions in the same way as for contact-only cards.

3.4 Ordering Cards

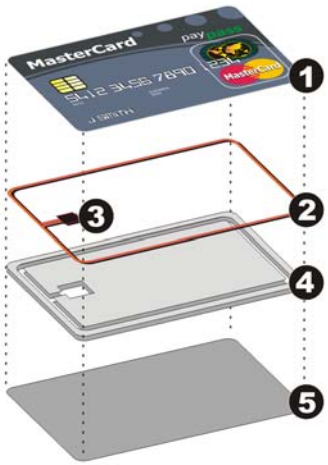
When ordering cards from a card manufacturer, the issuer must ensure that the card meets all MasterCard requirements. The issuer must ensure the card producer has the *PayPass* "Letter of Approval."

As well as being responsible for embedding the contactless (or dual-interface) chip into a MasterCard branded card, the card manufacturer (in the role of application provider) is responsible for putting the correct payment application onto the card.

The manufacturing process for a *PayPass* dual-interface card is different from that used for a contact card. Because of the added complexity in the production process, MasterCard has specific requirements for the mechanical robustness of the card. In addition to the "traditional" requirements such as minimum surface distortion and minimum bowing in cards, the following additional requirements need to be proven:

- Mechanical robustness of the dual-interface module
- Connectivity of the antenna

The different components of a dual-interface card are illustrated in Figure 4.



1. Card Laminate
2. Antenna
3. IC Chip
4. Inlay
5. Card Base

Figure 4, Card Schematics—Layers

In simple terms, the process is as follows:

- The chip manufacturer (or foundry) manufactures the chip and masks the operating system.
- The inlay provider provides white plastic with the antenna embedded. The combination of the white plastic with the antenna constitutes the inlay.
- The card manufacturer prints the overlay and laminates the different layers into printed plastic sheets. Also, the magnetic stripe and the signature field are added. Then, the card manufacturer has to mill and glue the module (with chip) in the plastic and bond the antenna to the module.
- The card manufacturer punches the sheets into individual cards.
- The cards are pre-personalized.

Each stage of the manufacturing process is validated and approved with a Card Quality Management (CQM) label.

A full *PayPass* card "Letter of Approval" is only granted to a card when:

- The product has all conformity statements.
- Each individual component has the required CQM Label.
- Compliance Assessment Security Testing (CAST) evaluation is complete.

3.5 *PayPass*—M/Chip Card Application

The *PayPass*—M/Chip application has been developed to work on chip cards that have two external interfaces: a contact and a contactless interface. This is a dual-interface application capable of performing transactions through both the contact and contactless interfaces with the restriction that a card can only use one interface at a time.

The following sections describe the impact of the processing features specific to the *PayPass*—M/Chip application.

3.5.1 *PayPass*—M/Chip Data Objects

The *PayPass*—M/Chip application is a dual-interface application maintaining three sets of data:

- Data objects for when the contact interface is used
- Data objects for when the contactless interface is used
- Common data objects used across both interfaces

The *PayPass*—M/Chip application has been developed in such a way that it knows at every stage of the transaction which set of data to use.

Most data objects are shared between the contact and contactless interface and need to be personalized only once. The persistent data objects that are not shared are the following:

- *Application Control*
- *Card Issuer Action Codes*
- *Application Interchange Profile (AIP)*
- *Application File Locator (AFL)*

When personalizing the additional *PayPass* data objects, the following must be taken into account:

- The *Card Issuer Action Codes (PayPass)* and *Application Control (PayPass)* must be configured to indicate that offline PIN is not supported over the contactless interface.
- The *AIP (PayPass)* must be configured to indicate that the card supports the *PayPass*—M/Chip profile. This automatically results in a different *Signed Static Application Data (SSAD)* for the contactless and contact interface.
- *The AFL (PayPass)* must be personalized with the predefined *PayPass* value. The fixed value for the *AFL (PayPass)* imposes constraints on the organization of the data objects into the files referenced in the *AFL*.

The personalization of the *PayPass* specific data objects is explained in more detail in Chapter 4, *Personalization of the PayPass—M/Chip Application.*

3.5.2 PayPass—M/Chip Application Behavior

Although the *PayPass*—M/Chip application processes transactions in both contact and contactless mode, there is different behavior across two interfaces. The specific circumstances where the application behaves differently are addressed below.

3.5.2.1 Application Selection

For *PayPass* contactless transactions, an efficient application selection mechanism has been designed. The list of Application Identifiers (AIDs) supported by the card is obtained from the card by means of the SELECT PPSE *(PayPass* Payment System Environment) command.

The PPSE mechanism is similar to the EMV PSE mechanism, but is optimized by including the list of AIDs directly in the *File Control Information* (*FCI)*. Every *PayPass* card must provide support for the PPSE.

The issuer must take into account the following limitations imposed by the PPSE mechanism:

- Application selection using a partial AID is not supported by the PPSE mechanism.
- The reader automatically selects the highest priority application. Interactive cardholder selection is not supported (adding to the speed and transaction convenience that *PayPass* provides). The reader will not select an application prohibiting selection without cardholder assistance (i.e., b8 = 1b in the *Application Priority Indicator [API]).*

3.5.2.2 Card Risk Management Counters

The *PayPass*—M/Chip application shares the offline risk management counters between the contact and contactless interface. There are no specific counters for the contactless interface.

3.5.2.3 Signed Data Authentication (SDA) and Combined Data Authentication (CDA)

PayPass—M/Chip does not support Dynamic Data Authentication (DDA). Only SDA and CDA are supported. This requirement impacts on the personalization of the *AIP* (tag '82').

DDA is not supported because:

- DDA is slightly slower than CDA because of the extra INTERNAL AUTHENTICATE command.
- CDA provides better security than DDA because it allows the card to sign the transaction-related data.

3.5.2.4 Offline Personal Identification Number (PIN)

PayPass—M/Chip does not support offline PIN verification over the contactless interface. Neither offline plain text PIN nor offline enciphered PIN verification are available. There are two reasons for not supporting offline PIN:

- Entering a PIN while holding the card in front of the reader is not practical.
- Eavesdropping and PIN probing.

Deactivating offline PIN support over the contactless interface requires specific personalization of the *Application Control (PayPass)*. Refer to Section 4.4, *Configuring the Application Control (PayPass)* for more details.

Not supporting offline PIN over the contactless interface also impacts the personalization of the *Cardholder Verification Method (CVM) List.* The *CVM List* for the contactless interface should not indicate support for offline PIN.

A different *CVM List* for the contact and contactless interface has the following impact:

- The organization of the data objects into the files referenced in the *AFL* must be adapted accordingly (refer to Section 4.2, *File Organization and AFL*).
- A different *SSAD* for the contact and contactless interface must be generated.

Note also that *PayPass* terminals do not support offline PIN. Therefore, even if the *CVM List* includes support for offline PIN, it will never be performed.

3.5.2.5 Online Processing

PayPass—M/Chip is mainly intended for low-value payments, approved offline by both card and terminal, giving a "tap-and-go" experience to the customer.

PayPass—M/Chip also supports online authorization. If the transaction goes online the customer cannot be expected to hold the card in the field long enough to receive a response from the issuer. Consequently, issuer authentication and script processing (or post-issuance updates) will not be done over the contactless interface. Issuer scripts will only be sent to the card during an online contact payment transaction.

As a consequence, the offline counters can only be reset after an online contact payment transaction, and the counters remain unchanged if a *PayPass*—M/Chip contactless transaction is completed online.

3.5.2.6 Cardholder Activated Terminal (CAT) Level 3

The *PayPass* card will normally use the contact interface (e.g., ATM) at regular intervals. The contact interface, in combination with the online capability of the terminal can then be used by the issuer to reset the offline counters in the card.

However, if cardholders use a *PayPass*—M/Chip card exclusively over the contactless interface, the card application may eventually reject offline transactions.

The issuer can deactivate card risk management for CAT Level 3 transactions. This allows cardholders to continue to do low-value contactless CAT Level 3 transactions. Refer to Section 4.4.2, *Card Issuer Action Code (CIAC)—Default on CAT3,* for more detail.

3.5.2.7 *PayPass*—Mag Stripe Processing

Interoperability between *PayPass*—Mag Stripe and *PayPass*—M/Chip requires both the *PayPass*—M/Chip card and terminal to support *PayPass*—Mag Stripe.

PayPass—Mag Stripe transactions are secured by Card Verification Code 3 (CVC3). The CVC3 may be dynamic or static.

- **Dynamic CVC3**

  In the case of dynamic CVC3, the card generates a CVC3 value specific to each transaction. The card creates CVC3 using (part of) the *Unpredictable Number (Numeric) (UN)* generated by the terminal and the *Application Transaction Counter (ATC).* The card returns the CVC3 value to the terminal. The terminal then populates *Track 1 and/or Track 2 Data* with (part of) the *UN*, (part of) the *ATC* and (part of) the CVC3. The impact of supporting dynamic CVC3 is twofold:

  - Issuers must modify their personalization system to generate, manage, and supply the *PayPass*—Mag Stripe specific personalization data. This includes the management of a new Triple–DES *Key (Integrated Circuit Card [ICC] Derived Key for CVC3 Generation)* which is currently not supported by the M/Chip 4 application. Section 4.7, *PayPass—Mag Stripe Data Objects*, details the personalization requirements for the *PayPass*—Mag Stripe specific personalization data.
  - Issuers must modify the Issuer Host System (IHS) to be able to verify the dynamic CVC3. Section 3.9.2, *Authorizing PayPass—Mag Stripe Transactions*, details the impact on the IHS.

- **Static CVC3**

  The *PayPass*—M/Chip application allows the deactivation of dynamic CVC3 generation and the use of a static CVC3 to complete a *PayPass*—Mag Stripe transaction. Use of the static CVC3 option allows the issuer to implement the *PayPass*—M/Chip application without having to change the IHS to support the *PayPass*—Mag Stripe functionality. With static CVC3, the transaction can be processed in the same way as current magnetic stripe transactions provided the same algorithm is used as for CVC1.

  MasterCard recommends the static CVC3 value should differ from the CVC1 value in the magnetic stripe's track data. An easy way to create a CVC3 value different from the CVC1 on the magnetic stripe without having to change the IHS, is to use a different Service Code for the *Track 1 Data* and *Track 2 Data* as part of the *PayPass*—Mag Stripe emulation. The Service Code for the *PayPass*—Mag Stripe emulation should be 202 (for international transactions) or 602 (for domestic transactions) while the Service Code on the magnetic stripe is 201 or 601.

The issuer must be aware that static CVC3 is significantly less secure than dynamic CVC3. The issuer should refer to the *PayPass—Mag Stripe Security Architecture* document as input to the risk assessment.

3.6 Multiapplication

Contactless technology is already widespread in non-payment environments such as ticketing, loyalty and identification, and access. There is no technical reason why non-payment applications cannot reside on *PayPass*—M/Chip cards, with *PayPass* being the first-choice payment application ("top-of-wallet"). *PayPass* multiapplication cards are readily available on the standard multiapplication platforms (MULTOS and JavaCard).

PayPass—M/Chip can cope with and is easily integrated with other legacy applications. The non-payment applications are often implemented on memory cards. In this scenario, *PayPass*—M/Chip does not require a multiapplication platform to support the nonpayment application. Depending on the technology, *PayPass*—M/Chip can "emulate" the nonpayment application at the level of the silicon (e.g., MIFARE emulation), without interfering with the *PayPass*—M/Chip application.

The challenge for multiapplication is the same as for contact, i.e., establishing the business and operational relationship with the nonpayment entity that has already deployed the contactless technology (e.g., mass transit, transport, toll-road operators). As the issuer and nonpayment applications will share the same space (i.e., the physical *PayPass* card), a service agreement needs to be established between the different partners (including the card issuer) covering roles and responsibilities for application loading, help desk, card replacement, etc.

3.7 Personalization

Although the *PayPass*—M/Chip application can be personalized over the contactless interface, it is more convenient to personalize it over the contact interface. The normal process for (contact) M/Chip 4 personalization can be used with a requirement for additional data. The issuer must prepare the additional data and ensure the card personalizer is fully aware of these values. The additional data are:

- The *FCI* of the PPSE containing the list of supported *AIDs.*
- The *PayPass*—M/Chip specific data objects: *Application Control (PayPass), Card Issuer Action Codes (PayPass), Application Interchange Profile (PayPass),* and *Application File Locator (PayPass)*.
- The additional data to support *PayPass*—Mag Stripe emulation.

As an additional step in the personalization process, the personalization equipment must check whether the contactless interface functions properly. Existing personalization equipment should be upgraded to include a contactless head that allows a link to be established with the card and to exchange data. When issuing *PayPass* cards, the issuer has the choice of either purchasing the appropriate module for checking the contactless interface or outsourcing the personalization task to a personalization bureau.

Chapter 4, *Personalization of the PayPass—M/Chip Application*, describes *PayPass*-specific personalization in detail. Appendix A, *PayPass Network Upgrade*, provides examples of *PayPass*-specific values for all the *PayPass*—M/Chip data objects that require personalization.

3.8 Card Delivery

PayPass data may be read by any reader that can power the contactless chip and send the correct commands. It is possible that card data could be captured while in transit to the customer. The issuer must determine if any special procedures are needed for the packaging and mailing of *PayPass* cards.

The issuer may consider putting electromagnetic shielding, such as aluminum foil, into the envelopes to mask the presence of a *PayPass* card. Without such shielding, identification of mail containing payment cards is possible and the risk of lost and stolen cards ("never arrived") may increase.

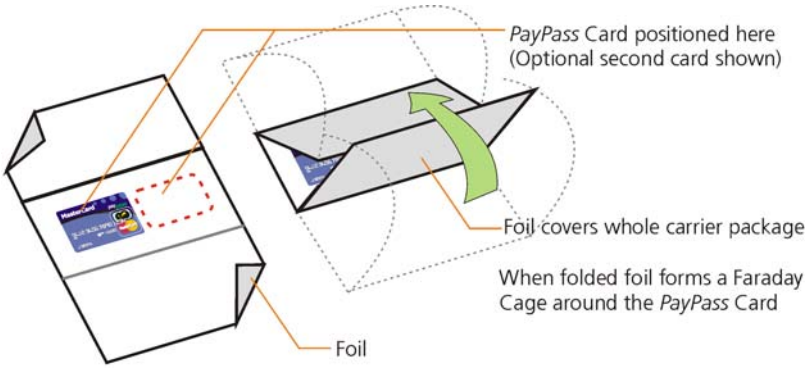

PayPass Card positioned here
(Optional second card shown)
Foil covers whole carrier package
When folded foil forms a Faraday
Cage around the *PayPass* Card
Foil

Figure 5, Carrier Manufactured from Aluminum Foil/Paper Laminate

NOTE

The issuer should refer to *Protecting MasterCard PayPass Cards and Devices in the Mail* for more details about protecting *PayPass* cards in the mail.

3.9 Issuer Host System (IHS)—Authorization

This section describes the impact of *PayPass* on the IHS for the authorization of *PayPass* transactions.

The issuer must support *PayPass* indicators in authorization messages and must be able to validate CVC3 for *PayPass*—Mag Stripe transactions.

3.9.1 Identifying the *PayPass* Profile

As *PayPass* is a new product, fraud patterns may differ from magnetic stripe and (contact) chip transactions. In order to clearly identify *PayPass* transactions, MasterCard has created new values for existing data elements to highlight *PayPass* transactions to the issuer (see Appendix A*, PayPass Network Upgrade*).

The different values contain sufficient information for the issuer to determine the type of card (*PayPass*—Mag Stripe or *PayPass*—M/Chip) and the type of terminal (*PayPass*—Mag Stripe or *PayPass*—M/Chip) involved in the transaction.

All *PayPass* transactions will be labeled with these specific values and the issuer must ensure the IHS can accept these values as part of the authorization messages.

In a first instance, an issuer can ignore these values and treat the transaction as regular magnetic stripe or contact M/Chip transactions, provided the issuer has taken a number of precautions when issuing the cards:

- For *PayPass*—M/Chip transactions, the cryptography should be the same for both contact and contactless transactions.
- For *PayPass*—Mag Stripe transactions, the cards should use static CVC3 with the same algorithm as used for CVC1.

NOTE

To check whether the IHS accepts *PayPass* values in the authorization, the issuer can use the MasterCard simulator. The simulator is provided with a contactless terminal. The issuer can connect the simulator to the IHS and present either the issuer's cards or MasterCard test cards.

3.9.2 Authorizing *PayPass*—Mag Stripe Transactions

A *PayPass*—M/Chip card used at a *PayPass*—Mag Stripe terminal will perform a *PayPass*—Mag Stripe transaction, so *PayPass*—M/Chip issuers must support *PayPass*—Mag Stripe cryptography on their IHS.

In the following sections verification of both static and dynamic CVC3 is addressed.

3.9.2.1 Dynamic CVC3 Verification

To verify the dynamic CVC3 the issuer must recalculate the dynamic CVC3 and compare it with the dynamic CVC3 included in the discretionary data field. Refer to the *PayPass—Mag Stripe Security Architecture* to determine how to validate the dynamic CVC3.

The recommendations below must be followed to ensure an appropriate level of security.

- The issuer must keep track of the entire *ATC* (i.e., must be able to find the complete *ATC* when receiving truncated *ATC* in the discretionary data).
- The issuer must decide on an appropriate strategy for managing and using the *ATC* (to avoid a denial of service attack).
- If the *CVC3* verified by the issuer is invalid, the issuer must decline the transaction. The issuer may wish to block the card with the next contact transaction.

Refer to the *PayPass—Mag Stripe Security Architecture* for a detailed description of each of the recommendations.

3.9.2.2 Static CVC3 Verification

With static CVC3, the transaction can be processed in the same way as current magnetic stripe transactions provided the same algorithm is used as for CVC1. The static CVC3 option allows the issuer to process *PayPass*—Mag Stripe transactions without any impact on the IHS.

NOTE

MasterCard recommends calculating the CVC1 using the DES method as described in *Security Rules and Procedures.*

3.9.3 Authorizing *PayPass*—M/Chip Transactions

When an online authorization is requested during a *PayPass*—M/Chip transaction, the *PayPass*—M/Chip application generates an Authorization Request Cryptogram (ARQC). Full-grade acquirers (i.e., where the acquirer supports the transfer of the ICC System-related Data in DE055) send the ARQC in the authorization request message along with the transaction data.

3.9.3.1 Verifying the ARQC

Full-grade issuers can authenticate *PayPass*—M/Chip payment transactions dynamically through the ARQC. The verification of the ARQC generated by the *PayPass*—M/Chip application is processed in the same way as the verification of an ARQC generated by the M/Chip 4 application. Refer to the *M/Chip 4 Security and Key Management* manual for details of ARQC verification.

3.9.3.2 Issuer Application Data

For the interpretation of the *Issuer Application Data* generated during a *PayPass*—M/Chip transaction, refer to the *PayPass—M/Chip 4 Issuer Guide for Debit and Credit Parameter Management.*

3.9.3.3 Issuer Authentication Data

The issuer must not generate *Issuer Authentication Data* for an online *PayPass*—M/Chip transaction, because the *PayPass* terminal is not able to pass it to the *PayPass* card.

The issuer sends the result of the authorization decision to the terminal (and not to the *PayPass* card) in DE039 (Response Code) in the same way as for magnetic-stripe transactions.

3.9.3.4 Script Processing

The issuer must not generate issuer scripts for an online *PayPass*—M/Chip transaction because the *PayPass* terminal is not able to pass them to the *PayPass* card.

3.9.3.5 Terminal Verification Results (TVR)

A *PayPass* terminal has a transaction flow optimized for speed. Offline data authentication and terminal risk management functions (checking of expiry date, floor limit, etc.) may be postponed by the terminal until the card has been removed from the field. In these situations, the terminal will send an "assumed" *TVR* to the card in the value field of the first GENERATE AC command.

The issuer must take into account that the *TVR* included in the authorization request does not always reflect the real outcome of the terminal tests.

3.10 Issuer Host System (IHS)—Clearing

This section describes the impact of *PayPass* on the IHS for the clearing of *PayPass* transactions.

3.10.1 Identifying the *PayPass* Profile

In the same way as for authorization, MasterCard has created new values for existing data elements to indicate *PayPass* transactions in the clearing data to the issuer.

The Service Code in the track data identifies whether the card is *PayPass*—M/Chip (value 2xx or 6xx) or *PayPass*—Mag Stripe (value 1xx or 5xx). DE022 indicates the terminal capabilities (*PayPass*—Mag Stripe or *PayPass*—M/Chip) as described in Appendix A, *PayPass Network Upgrade.*

All *PayPass* transactions will be labeled with these specific values and the issuer must ensure the IHS can accept these values in the clearing messages.

NOTE

To check whether the IHS accepts the *PayPass* values in the clearing, issuers can use the MasterCard simulator. This simulator is provided with a contactless terminal. Issuers can connect the simulator to the IHS and present either the issuer's cards or MasterCard test cards.

3.10.2 Clearing *PayPass*—Mag Stripe Transactions

The *PayPass*—Mag Stripe CVC3 value is not included in the clearing data. It is therefore irrelevant whether the *PayPass*—M/Chip application used static or dynamic CVC3 for the *PayPass*—Mag Stripe authorization. Therefore, *PayPass*—Mag Stripe transactions are cleared in the same way as traditional magnetic stripe transactions.

3.10.3 Clearing *PayPass*—M/Chip Transactions

While clearing *PayPass*—M/Chip transactions the following two points must be taken into account by the issuer:

- Where a *PayPass*—M/Chip transaction was approved online, the issuer must be aware that:
  - No second GENERATE AC was performed
  - DE055 contains the chip data generated by the first GENERATE AC

    This means that the *Card Verification Results* and *Cryptogram Information Data* will indicate that the *Application Cryptogram* is an ARQC.

    Where a *PayPass*—M/Chip transaction was approved offline, the *Card Verification Results* and *Cryptogram Information Data* will indicate that *Application Cryptogram* is a TC.
- As explained in Section 3.9.3.5, *Terminal Verification Results*, the issuer must take into account that the *TVR* included in the clearing record does not always reflect the real outcome of the terminal tests.

3.11 Issuer Testing

This section outlines the testing the issuer must perform before releasing *PayPass* into a live environment.

3.11.1 Card Validation

The card validation phase is designed to ensure that the issuer will deploy valid *PayPass* cards. It includes the following key services:

- Card Design Approval
- Card Personalization Validation

The Card Design Approval service validates that the card complies with MasterCard branding requirements. The main steps to the card design approval process include submission of:

- Preliminary designs (by issuer)
- Color proof (by vendor)
- Color sample cards (by vendor)

Full details of the process are provided in the *Card Design Standards* manual.

The Card Personalization Validation service includes extensive tests designed to validate that the parameters personalized on the card meet with MasterCard *PayPass* requirements. For more detailed information we refer to the *Card Personalization Validation Guide*.

3.11.2 Network Interface Validation

In order to correctly process *PayPass* transactions, issuers need to amend their network interfaces with MasterCard. The Network Interface Validation test stage is designed to prove network authorization request messages can be received, responses can be sent, and clearing files can be processed.

For authorization testing, issuers must use the appropriate version of the MasterCard Authorization Simulator (MasterINQ) to ensure that they are able to correctly process the *PayPass* data in the authorization messages.

The issuer may also include the clearing environment in the Network Interface Validation phase.

3.11.3 End-to-End Demonstration (ETED)

The ETED is designed to validate that *PayPass* cards and all systems under the control of the issuer (e.g., authorization and clearing systems) function correctly.

There are three main activities performed by MasterCard during the ETED:

- Use of live cards (provided by the issuer) to perform transactions at MasterCard-approved POS terminals in selected countries.
- Monitoring of transactions across the real-time authorization network and through the clearing and settlement process.
- Analysis of log files, after the end-to-end tests have been performed.

3.12 Staff Training

The issuer's customer service/help desk staff need to be trained to handle calls relating to *PayPass* cards. The issuer should formulate a marketing plan that informs of the benefits of this new technology and increased acceptance areas such as fast food. New marketing material needs to be developed to educate the cardholders.

4. PERSONALIZATION OF THE *PAYPASS*—M/CHIP APPLICATION

4.1 Introduction

This chapter includes a detailed description of the personalization values for the *PayPass*—M/Chip application data objects. It contains only the specific personalization requirements for the *PayPass*—M/Chip application. For more information about the configuration of the M/Chip 4 application data objects, refer to the *M/Chip 4 Issuer Guide for Credit and Debit Parameter Management*. See also Appendix B, *Data Objects Personalization Values*, for a complete list, with example values, of all *PayPass*—M/Chip data objects that require personalization.

4.2 File Organization and *AFL*

Files referenced in the *AFL* for the contactless interface (referenced as the *AFL [PayPass])*, must be organized as specified in this section. This allows a *PayPass* terminal to retrieve the data objects from the card with a minimum number of READ RECORD commands.

The first record of the file with SFI 1 must include the data objects necessary to perform the *PayPass*—Mag Stripe transactions. Table 1 lists the contents of record 1 of SFI 1.

TAG	DATA OBJECT
'9F6C'	*Mag Stripe Application Version Number*
'9F62'	*Track 1 Bitmap for CVC3 (PCVC3$_{TRACK1}$)*
'9F63'	*Track 1 Bitmap for UN and ATC (PUNATC$_{TRACK1}$)*
'56'	*Track 1 Data*
'9F64'	*Track 1 Nr of ATC Digits (NATC$_{TRACK1}$)*
'9F65'	*Track 2 Bitmap for CVC3 (PCVC3$_{TRACK2}$)*
'9F66'	*Track 2 Bitmap for UN and ATC (PUNATC$_{TRACK2}$)*
'9F6B'	*Track 2 Data*
'9F67'	*Track 2 Nr of ATC Digits (NATC$_{TRACK2}$)*
'9F68'	*Mag Stripe CVM List*

Table 1, Record 1 of SFI 1

Table 2 lists the data objects that must be included (if present) in Record 1 of the file with SFI 2. This record is the only record to be used as input for the generation of the *Signed Static Application Data*. This record may or may not be shared between the contact and contactless interface. If it is not shared, then the *SSAD* and the *ICC Public Key Certificate* will also not be shared.

TAG	DATA OBJECT
'57'	*Track 2 Equivalent Data*
'5A'	*Application Primary Account Number (PAN)*
'5F20'	*Cardholder Name*
'5F24'	*Application Expiration Date*
'5F25'	*Application Effective Date*
'5F28'	*Issuer Country Code*
'5F34'	*PAN Sequence Number*
'8C'	*CDOL1*
'8D'	*CDOL2*
'8E'	*CVM List*
'9F07'	*Application Usage Control*
'9F08'	*Application Version Number*
'9F0D'	*Issuer Action Code—Default*
'9F0E'	*Issuer Action Code—Denial*
'9F0F'	*Issuer Action Code—Online*
'9F42'	*Application Currency Code*
'9F4A'	*SDA Tag List*

Table 2, Record 1 of SFI 2

NOTE

Note that the *CVM List* for the contact mode and the contactless mode may still be the same and may indicate support for offline PIN. As *PayPass* terminals do not support offline PIN and the *Application Control (PayPass)* does not allow for PIN verification over the contactless interface, it is acceptable to use a common *CVM List*.

Table 3 and Table 4 list the data objects included in the first and second record of the file with SFI 3. These records must include the data objects required to retrieve the *Issuer Public Key* and to perform static data authentication.

TAG	DESCRIPTION
'8F'	*Certification Authority Public Key Index*
'9F32'	*Issuer Public Key Exponent*
'92'	*Issuer Public Key Remainder*
'90'	*Issuer Public Key Certificate*

Table 3, Record 1 of SFI 3

TAG	DESCRIPTION
'93'	*SSAD*

Table 4, Record 2 of SFI 3

Table 5 and Table 6 list the data objects required to retrieve the *ICC Public Key* and to perform dynamic data authentication. This file is only present for a *PayPass*—M/Chip Select application.

TAG	DESCRIPTION
'9F49'	Dynamic Data Object List (DDOL)
'9F47'	ICC Public Key Exponent
'9F48'	ICC Public Key Remainder

Table 5, Record 1 of SFI 4

TAG	DESCRIPTION
'9F46'	ICC Public Key Certificate

Table 6, Record 2 of SFI 4

Record 2 of SFI 3 *(SSAD)* and Record 2 of SFI 4 *(ICC Public Key Certificate)* can only be shared between the contact and contactless interface, if the following two conditions are fulfilled:

- Record 1 of SFI 2 is shared between the contact and contactless interface.
- Record 1 of SFI 2 does not include the *SDA Tag List.* If the *SDA Tag List* is included, then it must include the tag of the *AIP* (tag '82'). As the *AIP* is different for the contact and contactless interface, also the *SSAD* and *ICC Public Key Certificate* are different.

The predefined file structure for the contactless interface results in a fixed value for the *AFL (PayPass)*. For a *PayPass* M/Chip Lite application the *AFL (PayPass)* must be personalized with the value shown in Table 7.

SFI 1, REC# 1	SFI 2, REC# 1	SFI 3, REC# 1 & 2
08 01 01 00	10 01 01 01	18 01 02 00

Table 7, *AFL (PayPass)* for *PayPass*—M/Chip Lite

For an M/Chip Select dual interface application the *AFL (PayPass)* must be personalized with the value shown in Table 8.

SFI 1, Rec# 1	SFI 2, Rec# 1	SFI 3, Rec# 1 & 2	SFI 4, Rec# 1 & 2
08 01 01 00	10 01 01 01	18 01 02 00	20 01 02 00

Table 8, *AFL (PayPass)* for *PayPass*—M/Chip Select

The *AFL* used for the contact interface (referenced as the *AFL*) does not have the same restrictions and can be chosen freely in function of the records shared between contactless and contact interface.

The *PayPass*—M/Chip application does not interpret the data objects stored in the records included in the files with an *SFI* in the range from 1 to 10. These data objects are neither retrievable with the GET DATA command nor updateable with the PUT DATA command. Therefore, the same data object may occur in two different records with the same tag and a different value.

An example of how the data objects referenced in the *AFL* could be organized for a *PayPass*—M/Chip Select application is given in Table 11. This example uses a different *CVM List* for the contactless and contact interface. The data objects that are personalized with a different value are identified as *Data Object Name (Contactless)* and *Data Object Name (Contact)*.

For the example given in Table 11 the following two values for the *AFL (PayPass)* and *AFL* are used:

AFL (PayPass):

SFI 1, REC# 1	SFI 2, REC# 1	SFI 3, REC# 1 & 2	SFI 4, REC# 1 & 2
08 01 01 00	10 01 01 01	18 01 02 00	20 01 02 00

AFL:

SFI 2, Rec# 2	SFI 3, Rec# 1	SFI 4, Rec# 1	SFI 5, Rec# 1 & 2
10 02 02 01	18 01 01 00	20 01 01 00	28 01 02 00

Table 9, *AFL (PayPass)* and *AFL* for the *PayPass*—M/Chip Select Example

Although many of the data objects have the same value for the contactless and contact interface, they appear twice in two different records. As soon as one of the data objects in SFI 2, Record 1, cannot be shared, all the data objects in SFI 2, Record 1, must appear twice. In the example the data objects of SFI 2, Record 1, are repeated for the contact interface in SFI 2, Record 2.

In the example, the issuer uses the same *Issuer Public Key* and *ICC Public Key* for the contact and contactless interface. The *SSAD* and *ICC Public Key Certificate* can not be shared as the *CVM List* and the *AIP* have a different value for the contact and contactless interface.

NOTE

The *PAN* must be the same for the contact and contactless interface. A different *PAN* would result in different derived secret keys for AC generation and script processing which is not supported by the *PayPass*—M/Chip application.

The *AFL (PayPass)* and the *AFL* need a different tag because both data objects need to be accessible with the PUT DATA command during post-issuance processing.

The AFL has tag '94' for both the GET PROCESSING OPTIONS and PUT DATA commands. The AFL *(PayPass)* has tag '94' for the GET PROCESSING OPTIONS command and tag 'D9' for the PUT DATA command. Table 10 lists the tag values for the PUT DATA command.

Tag	Data Object
'94'	*AFL*

Tag	Data Object
'D9'	AFL *(PayPass)*

Table 10, *AFL* and *AFL (PayPass)* for PUT DATA

NOTE

Refer to Appendix B, *Data Objects Personalization Values,* for example values of the data objects listed in Table 11.

SFI 1		
REC.	**TAG**	**DESCRIPTION**
1	'9F66'	*PUNATC$_{TRACK2}$*
	'9F63'	*PUNATC$_{TRACK1}$*
	'56'	*Track 1 Data*
	'9F64'	*NATC$_{TRACK1}$*
	'9F65'	*PCVC3$_{TRACK2}$*
	'9F6C'	*Mag Stripe Application Version Number*
	'9F6B'	*Track 2 Data*
	'9F67'	*NATC$_{TRACK2}$*
	'9F68'	*Mag Stripe CVM List*

SFI 2		
1	'5F25'	*Application Effective Date*
	'5F24'	*Application Expiration Date*
	'9F07'	*Application Usage Control*
	'5A'	*PAN*
	'5F34'	*PAN Sec Nr*
	'9F0D'	*IAC—Default*
	'9F0E'	*IAC—Denial*
	'9F0F'	*IAC—Online*
	'57'	*Track 2 Equivalent Data*
	'9F08'	*Application Version Number*
	'5F20'	*Cardholder Name*
	'5F28'	*Issuer Country Code*
	'8C'	*CDOL1*
	'8D'	*CDOL2*
	'8E'	*CVM List (Contactless)*
	'9F42'	*Application Currency Code*
	'9F4A'	*SDA Tag List*
2	'5F25'	*Application Effective Date*
	'5F24'	*Application Expiration Date*
	'9F07'	*Application Usage Control*
	'5A'	*PAN*
	'5F34'	*PAN Sec Nr*
	'9F0D'	*IAC—Default*
	'9F0E'	*IAC—Denial*
	'9F0F'	*IAC—Online*
	'57'	*Track 2 Equivalent Data*
	'9F08'	*Application Version Number*
	'5F20'	*Cardholder Name*
	'5F28'	*Issuer Country Code*
	'8C'	*CDOL1*
	'8D'	*CDOL2*
	'8E'	*CVM List (Contact)*
	'9F42'	*Application Currency Code*
	'9F4A'	*SDA Tag List*

SFI 3		
REC.	**TAG**	**DESCRIPTION**
1	'8F'	*CA Public Key Index*
	'93'	*Issuer Public Key Certificate*
	'9F32'	*Issuer Public Key Exponent*
	'92'	*Issuer Public Key Remainder*
2	'93'	*Signed Static Application Data (Contactless)*

SFI 4		
1	'9F49'	*DDOL*
	'9F47'	*ICC Public Key Exponent*
	'9F48'	*ICC Public Key Remainder*
2	'9F46'	*ICC Public Key Certificate (Contactless)*

SFI 5		
1	'93'	*Signed Static Application Data (Contact)*
2	'9F46'	*ICC Public Key Certificate (Contact)*

Table 11, Example of a *PayPass*—M/Chip File Organization

4.3 Configuring the *AIP (PayPass)*

The *PayPass*—M/Chip application contains two instances of the *AIP (AIP* and *AIP [PayPass])*. The *AIP (PayPass)* includes the "M/Chip profile is supported" bit and must be personalized as specified in Table 12.

Byte 1 (leftmost):

b8	b7	b6	b5	b4	b3	b2	b1	MEANING
0								Reserved for Future Use (RFU)
	1							Offline static data authentication is supported
		0						Offline dynamic data authentication is supported
			1					Cardholder verification is supported
				1				Terminal risk management is to be performed
					0			Issuer authentication is supported
						0		RFU
							0/1*	Combined DDA—GENERATE AC supported

Byte 2 (rightmost):

b8	b7	b6	b5	b4	b3	b2	b1	MEANING
1								M/Chip profile is supported
	0	0	0	0	0	0	0	RFU

* 0b for M/Chip Lite 4, 1b for M/Chip Select 4.

Table 12, *AIP (PayPass)*

The *AIP (PayPass)* and the *AIP* need a different tag because both data objects need to be accessible with the PUT DATA command during post-issuance processing.

The *AIP* has tag '82' for both the GET PROCESSING OPTIONS and PUT DATA commands. The *AIP (PayPass)* has tag '82' for the GET PROCESSING OPTIONS command and tag 'D8' for the PUT DATA command.

Tag	Data Object
'82'	*AIP*

Tag	Data Object
'D8'	*AIP (PayPass)*

Table 13, *AIP* and *AIP (PayPass)* for PUT DATA

4.4 Configuring the *Application Control* (*PayPass)*

The *Application Control* data object activates or deactivates functions in the *PayPass*—M/Chip application. The *PayPass*—M/Chip application contains two instances of the *Application Control*. The *Application Control (PayPass)* and the *Application Control* have a different tag because both data objects need to be accessible with the PUT DATA and GET DATA commands during post-issuance processing.

Tag	Data Object
'D5'	*Application Control*

Tag	Data Object
'D7'	*Application Control* (*PayPass*)

Table 14, *Application Control* and *Application Control* (*PayPass)*

Table 15 describes the coding of the *Application Control (PayPass)*.

Byte 1:

b8	b7	b6	b5	b4	b3	b2	b1	MEANING
0/1								MagStripe grade issuer (0b: not activated, 1b: activated)
	0/1							Skip CIAC (*PayPass*)—default on CAT3 (0b: Do not skip CIAC (*PayPass*)—default, 1b: Skip CIAC *(PayPass)*—default)
		0						Reserved
			0					Key for offline encrypted PIN
				0				Offline encrypted PIN not supported
					0			Offline plain text PIN not supported
						0/1		Session key derivation (0b: MasterCard Proprietary SDK, 1b: EMV CSK)*
							0/1	Encrypt offline counters (0b: Do not encrypt, 1b: Encrypt)

* The definition of b2 used in this table is compatible with Option 2 as specified in *Addendum to M/Chip 4 Card Applications Specifications*.

Byte 2:

b8	b7	b6	b5	b4	b3	b2	b1	MEANING
0	0	0	0	0				Other values are RFU.
					0/1			Additional check table (0b: do not activate, 1b: activate)
						0/1		Retrieval of balance (0b: do not allow, 1b: allow)
							0/1	Include counters in AC (0b: do not include, 1b: include)

Byte 3:

b8	b7	b6	b5	b4	b3	b2	b1	DESCRIPTION
x								Indicate if *Static CVC3* must be used: • 0b: Do not use *Static CVC3* • 1b: Use *Static CVC3*
	x							Include *ATC* in *CVC3* generation: • 0b: Do not include *ATC* • 1b: Include *ATC*
		0	0	0	0	0	0	Other values are RFU

Table 15, *Application Control (PayPass)*

The following sections describe the setting of the bits related to specific requirements for the *PayPass* interface. For the setting of the other bits we refer to *the M/Chip 4 Issuer Guide for Credit and Debit Parameter Management*.

4.4.1 Mag Stripe Grade Issuer Activated

The application checks the "Mag Stripe Grade Issuer Activated" bit in the second GENERATE AC, when the *Issuer Authentication Data* is not present. If the "Mag Stripe Grade Issuer Activated" bit is set to 1, the card will be accepted when the *Issuer Authentication Data* is not present.

As the second GENERATE AC is not used for *PayPass* transactions, the "Mag Stripe Grade Issuer Activated" bit will also not be used and should be set to 0b.

4.4.2 Card Issuer Action Code (CIAC)—Default on CAT3

The application checks the "Skip CIAC—Default on CAT3" bit in the first GENERATE AC, when the terminal is a CAT level 3 terminal.

If the "Skip CIAC—Default on CAT3" bit is set to 1b, then the *PayPass*—M/Chip application skips the check on the *CIAC—Default* in the first GENERATE AC on a CAT Level 3 terminal. This allows the *PayPass*—M/Chip application to accept low-value transactions on CAT Level 3 terminals when offline limits are exceeded. This may be especially useful for the *PayPass*—M/Chip application where offline counters can only be reset during online contact payment transactions. Therefore the offline limits will probably be exceeded sooner than with an M/Chip 4 contact only application. By setting the "Skip CIA—Default on CAT3" bit to 1b in the *Application Control (PayPass)*, the cardholder will be able to continue performing low value transactions through the *PayPass* interface on CAT Level 3 terminals.

4.4.3 Key for Offline Encrypted PIN Verification

As offline encrypted PIN is not supported through the *PayPass* interface, the *PayPass*—M/Chip 4 application does not use the "Key for Offline Encrypted PIN Verification" of the *Application Control (PayPass)*. Therefore this bit must be set to 0b in the *Application Control (PayPass).*

4.4.4 Offline Encrypted PIN Verification

As offline encrypted PIN is not allowed through the *PayPass* interface, this bit must be set to 0b in the *Application Control (PayPass).* By setting this bit to 0b, the VERIFY PIN command will always return status bytes '6985'. This way PIN probing by a fraudulent terminal through the *PayPass* interface is impossible.

4.4.5 Offline Plain Text PIN Verification

As offline plain text PIN is not allowed through the *PayPass* interface, this bit must be set to 0b in the *Application Control (PayPass).* By setting this bit to 0b, the VERIFY PIN command will always return status bytes '6985'. This way PIN probing with a fraudulent terminal through the *PayPass* interface is impossible.

4.4.6 Static CVC3

Using this bit the *PayPass*—M/Chip application can deactivate the dynamic CVC3 generation and use a static CVC3 to complete a *PayPass*—Mag Stripe transaction.

4.4.7 Include *ATC*

When a dynamic CVC3 is used, this bit allows the *ATC* to be included or not in the dynamic CVC3 calculation during a *PayPass*—Mag Stripe transaction.

4.5 Configuring the CIACs (*PayPass*)

The *CIACs (PayPass)* are represented by three *PayPass*—M/Chip 4 proprietary data objects: *CIAC (PayPass)—Default*, *CIAC (PayPass)—Online* and *CIAC (PayPass)—Decline*. They are compared to the decisional part of the *Card Verification Results* to decide which cryptogram to include in response to the GENERATE AC command.

4.6 Configuring Card Risk Management Data Objects

Except for the *Application Control* and *CIACs* data objects, all other card risk management data objects are shared between the contact and contactless interface and need to be configured in the same way as for the M/Chip 4 application. Refer to *the M/Chip 4 Issuer Guide for Debit and Credit Parameter Management* for the description of the configuration of the data objects listed in Table 16.

TAG	DATA OBJECT
'C8'	*Card Risk Management (CRM) Country Code*
'C9'	*CRM Currency code*
–	*Currency Conversion Parameters*
'D1'	*Currency Conversion Table*
'9F14'	*Lower Consecutive Offline Limit*
'9F23'	*Upper Consecutive Offline Limit*
'CA'	*Lower Cumulative Offline Transaction Amount*
'CB'	*Upper Cumulative Offline Transaction Amount*
'D6'	*Default ARPC Response Code*
'D3'	*Additional Check Table*
–	*Card Data Object List (CDOL) 1 and CDOL 2 Related Data*
–	*Previous Transaction History*

Table 16, Card Risk Management Data Objects

4.7 *PayPass*—Mag Stripe Data Objects

Support of the COMPUTE CRYPTOGRAPHIC CHECKSUM command allows the *PayPass*—M/Chip application to be accepted on a *PayPass*—Mag Stripe terminal. The *PayPass*—Mag Stripe profile allows contactless payments to use authorization networks that presently support magnetic stripe authorizations. The *PayPass*—M/Chip application must store *Track 1* and *Track 2 Data*.

The track data sent to the issuer may be dynamic or static. In the case of dynamic track data, the discretionary data field contains a dynamic CVC3 that is generated by the *PayPass* card using a secret key, the ATC, and a UN generated by the terminal.

NOTE

The *Track 2 Data* (tag '9F6B') stored for *PayPass*—Mag Stripe is independent of the *Track 2 Equivalent Data* (tag '57') returned by the *PayPass*—M/Chip application during the read application data processing, both over the contact and contactless interface.

Table 17 lists the data objects that have to be configured to support the *PayPass*—Mag Stripe profile.

TAG	NAME
'56'	*Track 1 Data*
'9F62'	$PCVC3_{TRACK1}$
'9F63'	$PUNATC_{TRACK1}$
'9F64'	$NATC_{TRACK1}$
'9F65'	$PCVC3_{TRACK2}$
'9F66'	$PUNATC_{TRACK2}$
'9F67'	$NATC_{TRACK2}$
'9F68'	*Mag Stripe CVM List*
'9F69'	*Unpredictable Data Object List (UDOL)*
'9F6B'	*Track 2 Data*
'9F6C'	*Mag Stripe Application Version Number (Card)*
'DA'	Static $CVC3_{TRACK1}$
'DB'	Static $CVC3_{TRACK2}$
'DC'	$IVCVC3_{TRACK1}$
'DD'	$IVCVC3_{TRACK2}$

Table 17, *PayPass*—Mag Stripe Data Objects

4.7.1 Bitmaps

The *PayPass*—M/Chip application uses bitmaps to indicate positions in the discretionary data fields of the *Track 1 Data* and *Track 2 Data*. The following bitmaps are used:

- $PCVC3_{TRACK1}$ to indicate the position of the dynamic $CVC3_{TRACK1}$ in the discretionary data field of the *Track 1 Data*. The number of non-zero bits in $PCVC3_{TRACK1}$ is referred to as q_{TRACK1} and represents the number of dynamic $CVC3_{TRACK1}$ digits included in the discretionary data of the *Track 1 Data*.
- $PCVC3_{TRACK2}$ to indicate the position of the dynamic $CVC3_{TRACK2}$ in the discretionary data field of the *Track 2 Data*. The number of non-zero bits in $PCVC3_{TRACK2}$ is referred to as q_{TRACK2} and represents the number of dynamic $CVC3_{TRACK2}$ digits included in the discretionary data of the *Track 2 Data*.

- *PUNATC$_{TRACK1}$* to indicate the positions of *the UN (Numeric)* and *ATC* digits in the discretionary data field of the *Track 1 Data*. The number of non-zero bits in *PUNATC$_{TRACK1}$* is referred to as k_{TRACK1}. The symbol t_{TRACK1} represents the value of *NATC$_{TRACK1}$* and indicates the number of most significant positions in *PUNATC$_{TRACK1}$* reserved for the *ATC*. The least significant positions indicated in *PUNATC$_{TRACK1}$* are used for the *UN (Numeric)* digits. The number of *UN (Numeric)* digits is referred to as n_{UN} (= $k_{TRACK1} - t_{TRACK1}$).
- *PUNATC$_{TRACK2}$* to indicate the positions of the *UN (Numeric)* and *ATC* digits in the discretionary data field of the *Track 2 Data*. The number of non-zero bits in *PUNATC$_{TRACK2}$* is referred to as k_{TRACK2}. The symbol t_{TRACK2} represents the value of *NATC$_{TRACK2}$* and indicates the number of most significant positions in *PUNATC$_{TRACK2}$* reserved for the *ATC*. The least significant positions indicated in $PUNATC_{TRACK2}$ are used for the *UN (Numeric)* digits. The number of *UN (Numeric)* digits is referred to as n_{UN} (= $k_{TRACK2} - t_{TRACK2}$).

Figure 6 indicates the numbering of the different positions in the discretionary data. The number of digits present in discretionary data is indicated by m.

DISCRETIONARY DATA									
p_m	p_{m-1}	p_{m-2}	p_{m-3}	…	p_5	p_4	p_3	p_2	p_1

Figure 6, Numbering of Discretionary Data

Each bit in the bitmap refers to a position in the discretionary data. The least significant bit of the bitmap, i.e., the rightmost bit b_1, refers to position p_1 (as indicated in Figure 7). The number of bits in the bitmap is always a multiple of 8 and equal to q = (((m–1)/8)+1)*8. For the *Track 2 Data,* m_{TRACK2} is maximum 13 digits, resulting in a bitmap of 16 bits or 2 bytes. For the *Track 1 Data* the maximum value of m_{TRACK1} is 48, resulting in a bitmap of length 6 bytes or 48 bits.

					DISCRETIONARY DATA				
					p_m	p_{m-1}	p_{m-2}	p_{m-3}	…	p_5	p_4	p_3	p_2	p_1

b_q	b_{q-1}	b_{q-2}	…	b_{m+1}	b_m	b_{m-1}	b_{m-2}	b_{m-3}	…	b_5	b_4	b_3	b_2	b_1
BITMAP														

Figure 7, Relation between Discretionary Data and Bitmap

An example is given in Figure 8, for $m_{TRACK2} = 13$, $t_{TRACK2} = 2$ and $PUNATC_{TRACK2}$ = '031A', referring to position $p_{10}p_9p_5p_4p_2$. Based on this, k_{TRACK2} equals 5 and n_{UN} equals 3.

DISCRETIONARY DATA												
p_{13}	p_{12}	p_{11}	**p_{10}**	**p_9**	p_8	p_7	p_6	**p_5**	**p_4**	p_3	**p_2**	p_1

0	0	0	0	0	0	**1**	**1**	0	0	0	**1**	**1**	0	**1**	0
b_{16}	b_{15}	B_{14}	b_{13}	b_{12}	b_{11}	b_{10}	b_9	b_8	b_7	b_6	b_5	b_4	b_3	b_2	b_1
'0'				'3'				'1'				'A'			
BITMAP = '031A'															

Figure 8, Example $PUNATC_{TRACK2}$ = '031A'

4.7.2 *Track 2 Data*

The *Track 2 Data* contains the data objects of Track 2 according to [ISO/IEC 7813], excluding start sentinel, end sentinel, and LRC, as shown in Table 18.

DATA FIELD	FORMAT	LENGTH (NIBBLES)
Identification Number (PAN)	n	var. up to 19 digits
Field Separator (hex 'D')	b	1
Expiration Date (YYMM)	n	4
Service Code	n	3
Discretionary Data	n	variable length
Padded with hex 'F' to ensure whole bytes	b	0 or 1

Table 18, Track 2 Data

The discretionary data field of the *Track 2 Data* contains the placeholders for the dynamically generated $CVC3_{TRACK2}$, the t_{TRACK2} digits of the *ATC*, the n_{UN} digits of the *UN (Numeric)* and n_{UN} itself. All this data is copied into the discretionary data field by the terminal in the positions as indicated by the bitmaps. The dynamic $CVC3_{TRACK2}$ is generated by the *PayPass*—M/Chip application for each transaction and has to be verified by the issuer during the authorization processing. The digits of the discretionary data field at the positions not referred to in the bitmaps may be used by the issuer to store issuer proprietary data.

The following is an example of how the issuer may organize the discretionary data field of the *Track 2 Data*.

Example

PCVC3$_{TRACK2}$: '00 0E' ($\rightarrow q_{TRACK2} = 3$)
PUNATC$_{TRACK2}$: '0E 70' ($\rightarrow k_{TRACK2} = 6$)
NATC$_{TRACK2}$: '03' ($\rightarrow t_{TRACK2} = 3$ and $n_{UN} = 3$)
Track 2 Data: '54 13 12 34 56 78 48 08 D0 50 81 01 90 00 99 00 00 00 3F'

The discretionary data of the *Track 2 Data* contains the placeholders (zeroes in this example) for the *ATC, UN, CVC3$_{TRACK2}$*, and *n_{UN}* as follows:

```
9  000  99  000   000        3
   ↑↑↑     ↑↑↑   ↑↑↑        ↑
   ATC     UN    CVC3TRACK2 nUN
```

In this example, 10 digits out of 13 are used by the *PayPass* functionality. The remaining 3 digits can be used at the discretion of the issuer (the value 9 in this example).

4.7.3 *Track 1 Data*

The *Track 1 Data* contains the data objects of Track 1 according to ISO/IEC 7813 Structure B, excluding start sentinel, end sentinel, and LRC as shown in Table 19. The *Track 1 Data* has the alphanumeric special (ans) format and has to be ASCII encoded.

DATA FIELD	LENGTH (BYTES)
Format Code (hex '42' (B))	1
Identification Number (PAN)	variable up to 19
Field Separator (hex '5E' (^))	1
Name (see *[ISO/IEC 7813]*)	2 to 26
Field Separator (hex '5E' (^))	1
Expiration Date (YYMM)	4
Service Code	3
Discretionary Data	variable length

Table 19, *Track 1 Data*

The discretionary data field of the *Track 1 Data* contains the placeholders for the dynamically generated *CVC3$_{TRACK1}$*, the t_{TRACK1} digits of the *ATC*, the n_{UN} digits of the *UN (Numeric)* and n_{UN} itself. All this data is converted into ASCII format and copied into the discretionary data field by the terminal in the positions as indicated by the bitmaps. The dynamic *CVC3$_{TRACK1}$* is generated by the *PayPass*—M/Chip application for each transaction and has to be verified by the issuer during the authorization processing. The characters of the discretionary data field at the positions not referred to in the bitmaps may be used by the issuer to store issuer proprietary data.

NOTE

The length of the discretionary data field of the *Track 1 Data* may be much longer (up to 24 bytes for MasterCard products) than the length of the discretionary data field of the *Track 2 Data*. Therefore more static issuer proprietary data may be included.

The following is an example of how the issuer may organize the discretionary data field of the *Track 1 Data.*

Example

$PCVC3_{TRACK1}$:	'00 00 00 38 00 00' ($\rightarrow q_{TRACK1} = 3$)
$PUNATC_{TRACK1}$:	'00 00 00 00 E0 E0' ($\rightarrow k_{TRACK2} = 6$)
$NATC_{TRACK1}$:	'03' ($\rightarrow t_{TRACK2} = 3$ and $n_{UN} = 3$)
Track 1 Data:	'42 35 34 31 33 31 32 33 34 35 36 37 38 34 38 30 38 5E 53 4D 49 54 48 2F 4A 4F 48 4E 5E 30 35 30 38 31 30 31 33 33 30 30 30 33 33 33 30 30 30 32 32 32 32 32 30 30 30 31 31 31 31 30'
or ASCII dump:	B5413123456784808^SMITH/JOHN^050810133000333000 2222200011110

The discretionary data of the *Track 1 Data* contains the placeholders (zeroes in this example) for the *ATC, UN, $CVC3_{TRACK1}$,* and *n_{UN}* as follows:

33	000	333	000	22222	000	1111	0
	↑↑↑		↑↑↑		↑↑↑		↑
	$CVC3_{TRACK1}$		*ATC*		*UN*		*n_{UN}*

In this example 10 characters out of 24 are used by the *PayPass* functionality. The remaining 14 characters can be used at the discretion of the issuer.

4.7.4 *$IVCVC3_{TRACK1}$ and $IVCVC3_{TRACK2}$*

$IVCVC3_{TRACK1}$ and *$IVCVC3_{TRACK2}$* are two initialization vectors stored in the card during personalization and used by the *PayPass*—M/Chip application to generate the dynamic CVC3.

$IVCVC3_{TRACK1}$ is a MAC calculated over the static part of the *Track 1 Data* using the *ICC Derived Key for CVC3 Generation (KD_{CVC3}). $IVCVC3_{TRACK2}$* is a MAC calculated over the static part of the *Track 2 Data* also using *KD_{CVC3}.* Initialization vectors are used in order to protect the track data.

Refer to the *PayPass—M/Chip Technical Specification* for more details about the MAC computation.

4.7.5 *Static $CVC3_{TRACK1}$* and *Static $CVC3_{TRACK2}$*

The previous sections show that implementing the dynamic CVC3 may involve a significant amount of development for the issuer. To avoid this, *PayPass*—M/Chip issuers can use a static CVC3 instead. Control of CVC3 is achieved through a specific *Application Control (PayPass)* setting (refer to Section 4.4.6, *Static CVC3*) that deactivates the dynamic CVC3 generation.

4.7.6 *Mag Stripe CVM List*

The *PayPass*—M/Chip application returns a specific *CVM Lis*t for the *PayPass*—Mag Stripe transactions. For the MasterCard product there are two possibilities depending on the risk profile of the issuer: Signature + Online PIN + No CVM (Table 20) or Online PIN + Signature + No CVM (Table 21).

CVM	BIT 7 OF BYTE 1 IF CVM NOT SUCCESSFUL	BYTE 1 SETTING	BYTE 2 SETTING	MEANING OF BYTE 2
Signature	Apply next	'5E'	'03'	If supported
Online PIN	Apply next	'42'	'03'	If supported
No CVM	Fail	'1F'	'03'	If supported

Table 20, MasterCard—*Mag Stripe CVM List* (Signature + Online PIN + No CVM)

CVM	BIT 7 OF BYTE 1 IF CVM NOT SUCCESSFUL	BYTE 1 SETTING	BYTE 2 SETTING	MEANING OF BYTE 2
Online PIN	Apply next	'42'	'03'	If supported
Signature	Apply next	'5E'	'03'	If supported
No CVM	Fail	'1F'	'03'	If supported

Table 21, MasterCard—*Mag Stripe CVM List* (Online PIN + Signature + No CVM)

4.7.7 *Mag Stripe Application Version Number (Card)*

The *Mag Stripe Application Version Number (Card)* must be personalized with the value '00 01'.

Appendix A: *PayPass* Network Upgrade

PayPass Indication

Network messages for *PayPass* transactions include specific values in existing subelements to indicate the magnetic stripe equivalent data or the M/Chip data was supplied by a contactless chip.

These new field values are supported on Banknet and RSC Releases 04.1. From 1 January 2007, all *PayPass* transactions must include the correct field settings in MasterCard network messages.

Details of the above can be found in the following standard MasterCard publications available to MasterCard issuers and acquirers:

- "Banknet Release 04.1/RSC Release 04.1," Global Operations Bulletin No. 9, 2 September 2003, pp. 37–38
- "GCMS Release 04.1," Global Operations Bulletin No. 11, 3 November 2003, pp 8–10
- "MasterCard Credit Authorization Simulator Version 04.1," Global Operations Bulletin No. 1, 2 January 2004, pp. 42–43

Authorization Messages

For *PayPass* transactions, specific values in existing subelements within the authorization message will specify the terminal capability (DE061) and the mode of operation (DE022).

Table A-1 describes the *PayPass*-specific subelements that authorization messages will support.

DATA ELEMENT	SUBELEMENT	VALUE
061 (POS Data)	11 (POS card data terminal input capability)	• 4: contactless Mag Stripe • 3: contactless M/Chip
022 (POS Entry Mode)	1 (card data input capability)	• 91: PAN auto-entry via contactless Mag Stripe • 07: PAN auto-entry via contactless M/Chip

Table A-1, New Values for DE022 and DE061 for Authorization

Apart from the specific values to indicate *PayPass*, MasterCard *PayPass* transactions are authorized in the same way and using the same subelements as magnetic stripe or contact chip transactions.

Clearing Messages

As with authorization messages, specific values in existing subelements within the clearing messages will specify the terminal capability, and the mode of operation (input and output).

Table A-2 describes the *PayPass*-specific values of the subelements in the clearing messages.

DATA ELEMENT	SUBELEMENT	VALUE
022 (POS Entry Mode)	1 (card data input capability)	• A: terminal supports PAN auto-entry via contactless Mag Stripe • M: terminal supports PAN auto-entry via contactless M/Chip
022 (POS Entry Mode)	7 (card data input mode)	• A: PAN auto-entry via contactless Mag Stripe • M: PAN auto-entry via contactless M/Chip
022 (POS Entry Mode)	10 (card data output mode)	• 0: unknown no indication given • 1: none • 3: contactless Mag Stripe or M/Chip

Table A-2, New Values for DE022 for Clearing Message

Appendix B: Data Objects Personalization Values

Introduction

This appendix describes all the *PayPass*—M/Chip data objects that require personalization and provides an example for each of the data objects.

The example provides values for the following personalization profile:

1. M/Chip 4 Select
2. Full Chip—MasterCard
3. Offline Plain text PIN + Signature + Online PIN + No CVM for contact interface, Signature + Online PIN + No CVM for *PayPass* interface
4. No currency conversion
5. Dynamic CVC3, *ATC* included for *PayPass*—Mag Stripe profile

NOTE

These examples provide values for the *PayPass*—M/Chip 4 application supporting only the MasterCard Proprietary SKD (Refer to *M/Chip 4 Card Application Specifications*).

Persistent Data Objects for Application Selection

Table B-1 lists the persistent data objects for application selection. All data objects listed in Table B-1 are shared between the contactless and contact interface and need to be personalized only once with a value common for both interfaces.

DATA OBJECT	LENGTH	DESCRIPTION	EXAMPLE
AID	var.	The value must be the same as the value for the *DF Name* in the *FCI*.	'A0 00 00 00 04 10 10'
FCI	var.	Refer to *the PayPass—M/Chip Technical Specification*	'6F 17 84 07 A0 00 00 00 04 10 10 A5 0C 50 0A 4D 61 73 74 65 72 43 61 72 64'

Table B-1, Persistent Data Objects for Application Selection

Persistent Data Objects Referenced in the *AFL*

This section lists the persistent data objects that are included in the files referenced in the *AFL*. The data objects must be organized in the files with SFI 1 to 10 as described in Section 4.2, *File Organization and AFL.*

Table B-2 lists the *PayPass*—Mag Stripe specific data objects that are used to perform *PayPass*—Mag Stripe payment transactions.

TAG	DATA OBJECT	FORMAT	LENGTH (BYTES)	DESCRIPTION	EXAMPLE
'9F6C'	*Mag Stripe Application Version Number*	b	2	Version number assigned by the payment system for the specific application in the card	'00 01'
'9F62'	*Track 1 Bitmap for CVC3* (*$PCVC3_{TRACK1}$*) *	b	6	Refer to section 4.7.1.	'00 00 00 38 00 00'
'9F63'	*Track 1 Bitmap for UN and ATC* (*$PUNATC_{TRACK1}$*)*	b	6	Refer to section 4.7.1.	'00 00 00 00 E0 E0'
'56'	*Track 1 Data*	ans	Variable up to 76	Refer to section 4.7.3.	'56 3C 42 35 34 31 33 33 33 39 30 30 30 30 30 31 35 31 33 5E 53 4D 49 54 48 2F 4A 4F 48 4E 5E 31 32 30 37 32 30 31 33 33 30 30 30 33 33 33 33 30 30 30 32 32 32 32 32 30 30 30 31 31 31 31 30'
'9F64'	*Track 1 Nr of ATC Digits* (*$NATC_{TRACK1}$*)*	b	1	Refer to section 4.7.1.	'03'
'9F65'	*Track 2 Bitmap for CVC3* (*$PCVC3_{TRACK2}$*)	b	2	Refer to section 4.7.1.	'00 0E'
'9F66'	*Track 2 Bitmap for UN and ATC* (*$PUNATC_{TRACK2}$*)	b	2	Refer to Section 4.7.1.	'0E 70'
'9F6B'	*Track 2 Data*	b	Variable up to 19	Refer to Section 4.7.2.	'54 13 33 90 00 00 15 13 D1 20 72 01 90 00 99 00 00 00 0F'
'9F67'	*Track 2 Nr of ATC Digits* (*$NATC_{TRACK2}$*)	b	1	Refer to Section 4.7.1.	'03'
'9F68'	*Mag Stripe CVM List*	b	Variable up to 252	Refer to Section 4.7.6.	'00000000 00000000 5E03 4203 1F03'

*This data object must be present if *Track 1 Data* is present.

Table B-2, *PayPass*—Mag Stripe Data Objects Referenced in the *AFL*

Table B-3 lists the data objects stored in records referenced in the *AFL* that are used to perform M/Chip payment transactions.

Appendix B: Data Objects Personalization Values, continued

TAG	DATA OBJECT	FORMAT	LENGTH (BYTES)	DESCRIPTION	EXAMPLE
'9F42'	*Application Currency Code*	n 3	2	Refer to *the M/Chip Functional Architecture for Credit and Debit*	'09 78'
'5F25'	*Application Effective Date*	n 6	3	Refer to *the M/Chip Functional Architecture for Credit and Debit*	'04 01 01'
'5F24'	*Application Expiration Date*	n 6	3	Refer to *the M/Chip Functional Architecture for Credit and Debit*	'12 07 31'
'9F07'	*Application Usage Control*	b	2	Refer to *the M/Chip Functional Architecture for Credit and Debit*	'FF 00'
'5A'	*Application PAN*	Variable up to 19	Variable up to 10	Refer to *the M/Chip Functional Architecture for Credit and Debit*	'54 13 33 90 00 00 15 13'
'5F34'	*Application PAN Sequence Number*	n 2	1	Refer to *the M/Chip Functional Architecture for Credit and Debit*	'00'
'9F0D'	*Issuer Action Code—Default*	b	5	Refer to *the M/Chip 4 Issuer Guide for Credit and Debit Parameter Management*	'FC 50 A4 00 00'
'9F0E'	*Issuer Action Code—Denial*	b	5	Refer to *the M/Chip 4 Issuer Guide for Credit and Debit Parameter Management*	'04 00 08 00 00'
'9F0F'	*Issuer Action Code—Online*	b	5	Refer to *the M/Chip 4 Issuer Guide for Credit and Debit Parameter Management*	'F8 70 A4 98 00'
'9F08'	*Application Version Number*	b	2	Refer to *the M/Chip Functional Architecture for Credit and Debit*	'00 02'
'8C'	*CDOL 1*	b	Variable	M/Chip Lite 4: '9F02069F03069F1A0295055F2A029A039C019F37049F35019F4502 9F3403' M/Chip Select 4: '9F02069F03069F1A0295055F2A029A039C019F37049F35019F4502 9F4C089F3403'	'9F02069F03069F1A0295055F2A029A039C019F37049F35019F45029F4C089F3403'

Table B-3, M/Chip Data Objects Referenced in the *AFL*

TAG	DATA OBJECT	FORMAT	LENGTH (BYTES)	DESCRIPTION	EXAMPLE
'8D'	*CDOL 2*	b	Variable	M/Chip Lite 4: '910A8A029505' M/Chip Select 4: '910A8A0295059F37049F4C08'	'910A8A0295059F37049F4C08'
'5F20'	*Cardholder Name*	ans	2–26	Refer to *the M/Chip Functional Architecture for Credit and Debit*	'53 4D 49 54 48 20 4A 4F 48 4E'
'8E'	*CVM List*	b	Variable up to 252	Refer to section *the M/Chip 4 Issuer Guide for Credit and Debit Parameter Management*	Contact Interface: '0000000000000000 4103 5E03 4203 1F03' *PayPass* Interface: '0000000000000000 5E03 4203 1F03'
'5F28'	*Issuer Country Code*	n 3	2	Refer to *the M/Chip Functional Architecture for Credit and Debit*	'00 56'
'9F4A'	*SDA Tag List*	b	0 or 1	Refer to *the M/Chip 4 Security and key Management* If used, the only value allowed is '82'	'82'
'57'	*Track 2 Equivalent Data*	b	Variable up to 19	Refer to *the M/Chip Functional Architecture for Credit and Debit*	'54 13 33 90 00 00 15 13 D1 20 72 01 00 00 00 00 00 00'
'9F49'	*DDOL*	b	3	Must contain tag and length of *Unpredictable Number*.	'9F 37 04'
'8F'	*Certification Authority Public Key Index*	b	1	Refer to *the M/Chip 4 Security and key Management*	'F3'
'9F32'	*Issuer Public Key Exponent*	b	1–3	Refer to *the M/Chip 4 Security and key Management*	'03'
'92'	*Issuer Public Key Remainder*	b	$N_I - N_{CA} + 36$	Refer to *the M/Chip 4 Security and key Management*	'EFF4A554A084A829B0D6D5ACCC34B84C262B32436ABDAC9899308D51E57C83DF6908C389'

Table B-3, M/Chip Data Objects Referenced in the *AFL*, continued

Appendix B: Data Objects Personalization Values, continued

TAG	DATA OBJECT	FORMAT	LENGTH (BYTES)	DESCRIPTION	EXAMPLE
'93'	*SSAD*	b	N_I	Refer to *the M/Chip Functional Architecture for Credit and Debit* and *the M/Chip 4 Security and Key Management*	Contact interface: '8AF2025856930E80D4BADB5D4D9AE917E5503652B53A633F5D008FF98B902D89AD6166D87B0C99B5BF78117797F6D678FE54CB01162C0A6652B3FB3D807F2E3B34A5F9F9B43587ED4A78F278F30C49A300578CEC7DFFFB9031B82B239DF2976A8997A1C3951168E707774B3DA8D0F13B82F0087D0E34C5AF7B25E80D5464A069B2C67A2392FC00B22F991C167D56298F' *PayPass* interface: '36BCC5100C44125E66D30BFDF0271F69F8E51372C2034EA5C00E848A3DAD600802D22F4F51C875DC57D0A500F1B8EF0B15684EC900203651AB38BEFFC4C692B1D28963272387037CF1A053944AB6C1C1A1ACD1BF0673188420BBC57B5E96AF65367750175958160FC4D2885B61B738D621F6FB44BD991D2708850374D3AC71E6196859563BC24D3F808BF2C4BDD51AB9'
'90'	*Issuer Public Key Certificate*	b	N_{CA}	Refer to *the M/Chip 4 Security and Key Management*	'14E5B069954E7897C433F50D8C68399A3BE8A7E5B8334615E4FE9A8D153486C9087747E32A17A9FCA405F28237138870886F58B55A8067133DF088B96E99BB7E28F319464EC347F15EB4869E5FB29335CA89CA7227A1E6D82353A7E24DEF855F71C699CC95D59019479C95E7A22E7C2D379F886B704739CBFDDE4796F0006EB0180D6B77BD87AEFC44DD151A7E751DA2'
'9F47'	*ICC Public Key Exponent*	b	1–3	Refer to *the M/Chip 4 Security and Key Management*	'03'
'9F48'	*ICC Public Key Remainder*	b	N_{IC} - N_I + 42	Refer to *the M/Chip 4 Security and Key Management*	'D529BCACA7F9ECEADE85990F1E04FEAE9FA033DF691268F9F2D5'

Table B-3, M/Chip Data Objects Referenced in the *AFL*, continued

TAG	DATA OBJECT	FORMAT	LENGTH (BYTES)	DESCRIPTION	EXAMPLE
'9F46'	*ICC Public Key Certificate*	b	N_I	Refer to *the M/Chip 4 Security and Key Management*	Contact interface: '11BA41629773B18143C01F FE297351E574AD2B35851BB 0F70E117BAAE31EF97C78F5 026871CC383B3FBE0BDD41 21996718492F3AC599B553F 1898A9574BCF96C89276AE B9443DC02527703533589C 5AAD5B0B4DEE18FB860194 8BB8C771F0123696B5DEA7 D4AB0D329FC4ACCE7BB80E 04CD1F1B7FD524AF0202C9 9A1796189F7AD53C4EA5B3 AC22651A0B15C8D0380C7' *PayPass* interface: '498171D72BB6E2A94D486E 9DCB3589AA78BA98D1F542 C34DED7D97B9F7EE19DD36 8596EABE355C60E0592F004 BF292689035E89E0DC61575 A911DA8AC93E043431DC7 3C87E612FCF3A55C13AED1 431C72D4BAA48A009593B A8AA31FED4F04C6A555868 9AE752EEBE18B76D9469D0 AA846CFF6C92E22001E1F9 CB7CE4F464AD5F8DDF64E9 12D555754D08695CA9AFA9 C1'

Table B-3, M/Chip Data Objects Referenced in the *AFL*, continued

If offline encrypted PIN verification is supported by the contact interface and if the RSA key for PIN decryption is not the RSA key for signature generation, the data objects listed in Table B-4 are also stored in records referenced in the *AFL*. These data objects should not be stored in records referenced in the *AFL (PayPass)*.

Appendix B: Data Objects Personalization Values, continued

TAG	DATA OBJECT	FORMAT	LENGTH (BYTES)	DESCRIPTION	EXAMPLE
'9F2E'	*ICC PIN Encipherment Public Key Exponent*	b	1–3	Refer to *the M/Chip 4 Security and Key Management*	–
'9F2F'	*ICC PIN Encipherment Public Key Remainder*	b	$N_{PE} – N_I + 42$	Refer to *the M/Chip 4 Security and Key Management*	–
'9F2D'	*ICC PIN Encipherment Public Key Certificate*	b	N_I	Refer to *the M/Chip 4 Security and Key Management*	–

Table B-4, Additional Data Objects Referenced in the *AFL* for Offline Encrypted PIN Verification with a Dedicated Key

Persistent Data Objects for Card Risk Management

Table B-5 lists the persistent data objects for card risk management. Except for the *Application Control*, all data objects in Table B-5 are shared between the contact and contactless interface.

TAG	DATA OBJECT	FORMAT	LENGTH (BYTES)	DESCRIPTION	EXAMPLE
'D5'	*Application Control*	*b*	*2*	Refer to *the M/Chip 4 Issuer Guide for Credit and Debit Parameter Management*	'C4 00'
'D7'	*Application Control (PayPass)*	*b*	*2*	Refer to Section 3.4	'C0 00 40'
'D6'	*Default ARPC Response Code*	*b*	*2*	Refer to *the M/Chip 4 Issuer Guide for Credit and Debit Parameter Management*	'00 12'
'9F14'	*Lower Consecutive Offline Limit*	*b*	*1*	Refer to *the M/Chip 4 Issuer Guide for Credit and Debit Parameter Management*	'01 14'
'9F23'	*Upper Consecutive Offline Limit*	*b*	*1*	Refer to *the M/Chip 4 Issuer Guide for Credit and Debit Parameter Management*	'01 64'
'CA'	*Lower Cumulative Offline Transaction Amount*	*b*	*6*	Refer to *the M/Chip 4 Issuer Guide for Credit and Debit Parameter Management*	'00 00 00 01 00 00'
'CB'	*Upper Cumulative Offline Transaction Amount*	b	6	Refer to *the M/Chip 4 Issuer Guide for Credit and Debit Parameter Management*	'00 00 00 10 00 00'

Table B-5, Persistent Data Objects for Card Risk Management

TAG	DATA OBJECT	FORMAT	LENGTH (BYTES)	DESCRIPTION	EXAMPLE
'C4'	*Card Issuer Action Code—Default*	b	3	Refer to *the M/Chip 4 Issuer Guide for Credit and Debit Parameter Management*	'09 50 00'
'C5'	*Card Issuer Action Code—Online*	b	3	Refer to *the M/Chip 4 Issuer Guide for Credit and Debit Parameter Management*	'09 FB 00'
'C3'	*Card Issuer Action Code—Decline*	b	3	Refer to *the M/Chip 4 Issuer Guide for Credit and Debit Parameter Management*	'00 00 00'
'CD'	*Card Issuer Action Code—Default*	b	3	Refer to Section 4.5	'00 50 00'
'CE'	*Card Issuer Action Code—Online*	b	3	Refer to Section 4.5	'00 FB 00'
'CF'	*Card Issuer Action Code—Decline*	b	3	Refer to Section 4.5	'00 00 00'
'C9'	*CRM Currency Code*	b	2	Refer to *the M/Chip 4 Issuer Guide for Credit and Debit Parameter Management*	'09 78'
'D1'	*Currency Conversion Table*	b	25	Refer to *the M/Chip 4 Issuer Guide for Credit and Debit Parameter Management*	'0000000000 0000000000 0000000000 0000000000 0000000000'
'D3'	*Additional Check Table*	b	18	Refer to *the M/Chip 4 Issuer Guide for Credit and Debit Parameter Management*	'000000000000000000'
'C8'	*CRM Country Code*	n 3	2	Refer to *the M/Chip 4 Issuer Guide for Credit and Debit Parameter Management*	'00 56'
'C7'	*CDOL 1 Related Data Length*	b	1	Refer to *the M/Chip 4 Issuer Guide for Credit and Debit Parameter Management*	'2B'

Table B-5, Persistent Data Objects for Card Risk Management, continued

Appendix B: Data Objects Personalization Values, continued

Triple–DES Keys

Table B-6 lists the Triple–DES key for ICC dynamic number generation. The Triple–DES key listed in Table B-6 is shared between the contact and contactless interface.

TAG	DATA OBJECT	FORMAT	LENGTH (BYTES)	DESCRIPTION	EXAMPLE
–	*ICC Dynamic Number Master Key (MK_{IDN})*	b	16	Refer to *the M/Chip 4 Security and Key Management*	'34EF267957E9EC5104FB43D63751071C'

Table B-6, Triple–DES Key for ICC Dynamic Number Generation

Table B-7 lists the Triple–DES keys for MCI and EMV2000 session key derivation. All the Triple–DES keys listed in Table B-7 are shared between the contact and contactless interface.

TAG	DATA OBJECT	FORMAT	LENGTH (BYTES)	DESCRIPTION	EXAMPLE
–	*SM for Integrity Master Key (MK_{SMI})*	b	16	Refer to *the M/Chip 4 Security and Key Management*	'FD8C5EEF5E01319D98808C25C416732C'
–	*SM for Confidentiality Master Key (MK_{SMC})*	b	16	Refer to *the M/Chip 4 Security and Key Management*	'89CEFEDC68BAEF68851076978F5E2070'
–	*AC Master Key (MK_{AC})*	b	16	Refer to *the M/Chip 4 Security and Key Management*	'B5DA8C6123075213573EFD0870BCB349'

Table B-7, Triple–DES Master Keys for EPI/MCI and EMV 2000 Session Key Derivation

Table B-8 lists the Triple–DES Key for CVC3 Generation. This key is only used for *PayPass*—Mag Stripe transactions.

TAG	DATA OBJECT	FORMAT	LENGTH (BYTES)	DESCRIPTION	EXAMPLE
–	*ICC Derived Key for CVC3 Generation (KD_{CVC3})*	b	16	Refer to *[MCPTS]*	'3A0EE06EC8FE00919B3121B24FB08F51'

Table B-8, ICC Derived Key for CVC3 Generation

Table B-9 lists the Triple–DES Issuer Master Keys. The Issuer Master Keys must be diversified with the *PAN* and *PAN Sequence Number* to give the derived keys to be stored in the card. The Issuer Master Keys themselves are not stored in the card. They have the same value for the contact and contactless interface.

TAG	DATA OBJECT	FORMAT	LENGTH (BYTES)	DESCRIPTION	EXAMPLE
–	*Issuer Master Key for AC (IMK_{AC})*	b	16	Refer to *the M/Chip 4 Security and Key Management*	'9E15204313F7318ACB79B90BD986AD29'
–	*Issuer Master Key for SM for Integrity (IMK_{SMI})*	b	16	Refer to *the M/Chip 4 Security and Key Management*	'4664942FE615FB02E5D57F292AA2B3B6'
–	*Issuer Master Key for SM for Confidentiality (IMK_{SMC})*	b	16	Refer to *the M/Chip 4 Security and Key Management*	'CE293B8CC12A977379EF256D76109492'
–	*Issuer Master Key for ICC Dynamic Number (IMK_{IDN})*	b	16	Refer to *the M/Chip 4 Security and Key Management*	'94C53A6B14057DCBE5407F41B4ABFB80'
–	*Issuer Master Key for CVC3 Generation (IMK_{CVC3})*	b	16	Refer to *the M/Chip 4 Security and Key Management*	'01234567899876543210012345678998'

Table B-9, Triple–DES Master Keys

Miscellaneous

Table B-10 lists other persistent data objects.

TAG	DATA OBJECT	FORMAT	LENGTH (BYTES)	VALUE	EXAMPLE
–	*Key Derivation Index*	b	1	Refer to *the M/Chip 4 Security and Key Management*	–
'9F7E'	*Application Life Cycle Data*	b	48	Refer to Appendix A of *the M/Chip 4 Card Application Specifications for Credit and Debit.* Depending on the possible separation between the loading of the application code and the personalization data on the hardware, only part of the *Application Life Cycle Data* may be personalized.	–
'9F4F'	*Log Format*	b	Variable	The content of records in the Log of Transactions.	'9F4F119F27019F02065F2A029A039F36029F5206'

Table B-10, Miscellaneous Persistent Data Objects

Appendix B: Data Objects Personalization Values, continued

Get Processing Options Response

Table B-11 lists the persistent data objects for the GET PROCESSING OPTIONS response. Both the *AIP* and *AFL* must be personalized with a value for the contact interface and a value for the contactless interface.

TAG	DATA OBJECT	FORMAT	LENGTH (BYTES)	DESCRIPTION	EXAMPLE
'94'	*Application File Locator*	b	Variable. The length of the *AFL* depends on the organization of data objects in records. The record capacity, and therefore the memory needed for the *AFL*, is specific to each implementation.	The value must be consistent with the organization of data into records in files with SFI 1 to 30.	'10020201 18010100 20010100 28010200'
'82'	*Application Interchange Profile*	b	2	Refer to *the M/Chip 4 Issuer Guide for Credit and Debit Parameter Management*	'79 00'
'D9'	*Application File Locator (PayPass)*	b	12 for M/Chip Lite 4 16 for M/Chip Select 4	M/Chip Lite 4: '080101001001 010118010200' M/Chip Select 4: '080101001001 0101180102002 0010200'	'08010100 10010101 18010200 20010200'
'D8'	*Application Interchange Profile (PayPass)*	b	2	Refer to Section 4.3.	'59 80'

Table B-11, Persistent Data Objects for the Get Processing Options Response

Counters and Previous Transaction

Table B-12 lists those persistent data objects that are linked to the counters and keep track of previous transaction history. All the data objects listed in Table B-12 are shared between the contact and contactless interface.

TAG	DATA OBJECT	FORMAT	LENGTH (BYTES)	DESCRIPTION	EXAMPLE
–	*Application Transaction Counter Limit*	b	2	'FFFF' recommended	'FFFF'
–	*Previous Transaction History*	b	1	Refer to *the M/Chip 4 Issuer Guide for Credit and Debit Parameter Management*	'00'
–	*MAC in Script Counter Limit*	b	1	'0F' recommended	'0F'
–	*Global MAC in Script Counter Limit*	b	3	'FFFFFF' recommended	'FFFFFF'
–	*Bad Cryptogram Counter Limit*	b	2	'FFFF' recommended	'FFFF'

Table B-12, Persistent Data Objects for Counters and Previous Transaction

PIN Information

Table B-13 lists the persistent data objects for PIN information. The data objects in this section are only relevant for the contact interface and not used by the contactless interface.

TAG	DATA OBJECT	FORMAT	LENGTH (BYTES)	VALUE	DESCRIPTION
'9F17'	*PIN Try Counter*	b	1	'0x' Issuer specific, generally the initial value is the *PIN Try Limit*	'03'
–	*PIN Try Limit*	b	1	'0x' Issuer specific	'03'
–	*Reference PIN*	b	8	See below.	'26 12 34 56 FF FF FF FF'

Table B-13, Persistent Data Objects for PIN Information

The *Reference PIN* is stored in a PIN block. The format of the PIN block is the following:

C	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F

where:

- C (Control field) value is binary 2 ('0010b')
- N (PIN length) 4-bit binary number with permissible values of '0100b' to '1100b'
- P (PIN digit) 4-bit field with permissible values of '0000b' to '1001b'
- P/F (PIN/filler) Determined by PIN length
- F (Filler) 4-bit binary number with value of '1111b'

Appendix B: Data Objects Personalization Values, continued

Data Objects with a Fixed Initial Value

Table B-14 lists data objects with a fixed initial value. The decision about whether to include these data objects as data to be personalized is implementation-specific. If these data objects cannot be personalized, their initial values must be as specified in Table B-14. All data objects included in Table B-14 are shared between the contact and contactless interface.

TAG	DATA OBJECT	FORMAT	LENGTH (BYTES)	INITIAL VALUE
–	*Cumulative Offline Transaction Amount*	n 12	6	'000000000000'
–	*Consecutive Offline Transactions Number*	b	1	'00'
'9F5F'	*Script Counter*	b	1	'00'
–	*Log of the Current Transaction x (x = 1…10 or more)*	b	20	'00…00'
'9F36'	*Application Transaction Counter*	b	2	'0000'
–	*Global MAC in Script Counter*	b	3	'000000'
–	*Bad Cryptogram Counter*	b	2	'0000'

Table B-14, Data Objects with a Fixed Initial Value

Compute Cryptographic Checksum Related Data Objects

Table B-15 lists the data objects related to the COMPUTE CRYPTOGRAPHIC CHECKSUM command that have to be personalized. The data objects in this section are only relevant for the contactless interface and are not used by the contact interface.

TAG	DATA OBJECT	FORMAT	LENGTH (BYTES)	VALUE	EXAMPLE
–	*Static* $CVC3_{TRACK1}$	b	2	Refer to Section 4.7.5.	'00 00'
–	*Static* $CVC3_{TRACK2}$	b	2	Refer to Section 4.7.5.	'00 00'
–	$IVCVC3_{TRACK1}$	b	2	Refer to Section 4.7.4.	'C1 82'
–	$IVCVC3_{TRACK2}$	b	2	Refer to Section 4.7.4.	'54 1F'

Table B-15, Compute Cryptographic Checksum Related Data Objects

RSA Keys

This section lists the RSA keys. The RSA keys are shared between the contact and contactless interface. Table B-16 lists the RSA key information that must be stored in the card. The remainder of this section contains the detailed RSA key information used for the example.

TAG	DATA OBJECT	FORMAT	LENGTH (BYTES)	DESCRIPTION	EXAMPLE
–	*Length of ICC Public Key Modulus (N_{IC})*	b	1	Refer to *the M/Chip 4 Security and Key Management*	'80'
–	*ICC Private Key*	b	IS*	Refer to *the M/Chip 4 Security and Key Management*	(see below ICC RSA Key (128 bytes))
–	*Length of ICC PIN Encipherment Public Key Modulus (N_{PE})*	b	1	Refer to *the M/Chip 4 Security and Key Management*	–
–	*ICC PIN Encipherment Private Key*	b	IS*	Refer to *the M/Chip 4 Security and Key Management*	–

* Implementation specific

Table B-16, RSA Keys

The personalization of the *Length of ICC PIN Encipherment Public Key Modulus (N_{PE})* and the *ICC PIN Encipherment Private Key* may be optional on some implementations but must be consistent with the value set for the *Application Control* at personalization.

The following RSA keys have been used for the generation of the certificates in the example.

Certification Authority RSA Key (144 bytes)

Modulus:
'98F0C770F23864C2E766DF02D1E833DFF4FFE92D696E1642F0A88C5694C6479D16DB1537BFE29E4FDC
6E6E8AFD1B0EB7EA0124723C333179BF19E93F10658B2F776E829E87DAEDA9C94A8B3382199A350C0
77977C97AFF08FD11310AC950A72C3CA5002EF513FCCC286E646E3C5387535D509514B3B326E1234F
9CB48C36DDD44B416D23654034A66F403BA511C5EFA3'

Exponent:
'03'

Private Exponent:
'197D7692D30966207BE67A8078515DFAA8D551879192590B281C1763C3766144D92483894AA5C50
D4F67BD172A2F2D1EA70030BDB4B332E99FD9A6DFD810EC87E93D15C516A47CF15F944D7B42D9922
C57061F701A01C55AA381CDBC43C2F95755BC9CB31D6AA0514AEB598415FE10C714059CBBA45A93
E56F3A0F3410FF0835FFFB01D28D2F208CF8E44D378C761457'

Private Key Split for CRT:

Factor Q:
'C213EF8652145002FA71BE1D6926C218EBF323CC4FF4B87947D6A3AC3CB12D3DE8ECD373DE13355B
A738CBE66C2471A7C27CC1239F4637A2A43E9006D7847D590AD8725D9584B95F'

Factor P:
'C9BCCAC99EEBDD280770FEB9C4499CD03C133AD4E2CA16A6F262B05007E30DA67DFD77E1DA4BED
4D3DF61CC86D6F3DD8C576805886F674EDA720D22D3EA0F3FF8F0DF9FA317CBC3D'

P^-1 mod Q:
'BAA2F7CAFFC10B287EDC090A323D32CA175B89790E71DA6AB62BCA05F5C5E291F819803AE242C16
964AB682CC81A646DFC3DA0774903E58592640A98AE355B02626E80F4E09F5FDD'

Appendix B: Data Objects Personalization Values, continued

Q^-1 mod P:
'07BC267B4B279E99F6584A284CC0A0957F92858EDE571AE6ADE8B46AF54C84D44A67535172963846186AAED9A9E67643637DD74D0393C8ABAA4205BDF5B2B2FF8DFE702CFB1046E5'

Exp mod Q:
'81629FAEE162E001FC4BD4139B6F2C109D4CC288354DD050DA8F17C828761E2945F337A2940CCE3D1A25DD4448184BC52C532B6D14D97A6C6D7F0AAF3A585390B1E5A193B903263F'

Exp mod P:
'867DDC8669F2937004F5FF2682DBBDE0280CD1E341DC0F19F6EC758AAFECB3C453FE4FEBE6DD48DE294EBDDAF39F7E9083A4559059F9A3491A15E1737F15F7FFB4B3FBFC20FDD2D3'

Issuer RSA Key (144 bytes)

Modulus:
'A078BEB21E7BEE9F85F18E15F1ABB842556A33F84390236605C57C9AAA8127CC7E9C33FBF81894BBA0F53C7D1DE61D64E7C061F1689B1B21D91F0E10A5FD9AB0FCDFC06B5D860968F34D1D04FF6770E533661196B45F219500C9B10B18B71A1464BF6B673C19D432FCB8AB44EFF4A554A084A829B0D6D5ACCC34B84C262B32436ABDAC9899308D51E57C83DF6908C389'

***Exponent*:**
'03'

Private Exponent:
'02ACADD84D4EDD93B9B2F5916EB1CB9AB49FA2FFDEFE22B92AC34A9C2D822710354F6744331179F20F7B8DCEE2A1B3B09D7668084A46DA0D5D37FBF7BE7FF5C7376A2112DB28A24A418F5AA1B6E4FE1871D19A0A5ACB3E03DF2D6F141C0C2B66375E5208BBB2F59FDD531063001A330CEB9977DECDEFD04B4D83CB0A09446864BB46F5852CCDA1E0B836B93016F99D6B'

Private Key Split for CRT:

Factor Q:
'C29C4EB550B0209B544E5FCFBF62FAE09D28CE4FBC051B3411E7FCF6032C3F0F9922DF47E8F60BB99570B5A3EA736F67C264AA73C09B9B665961FC1FFA6754EA5C60C888CEA52B21'

Factor P:
'D3179068D10BC28F31F79759AD599DCC14FADA04C9D7D2EB58BC34653AFC03AB841DF4C900DAA293D31BDA4D822E949EDEEC777E39871F412CBA25421E9747BC5C48541137E2B369'

P^-1 mod Q:
'7C42DEDB0AF6AC9EFE9444716B7260252BCF9B6DDAB5DBB0932D23205C7C1DB19DB0AADB89868430812A2B3DF818959767E4A5CFADC0F9F1E957A4758893CAFA51A5030C6CD21632'

Q^-1 mod P:
'4C4EA5A3C9B047FBC957E80D5410ABEBF36D828146BCF322A1766860D1C90D426B664B5BF26DB0C6F86DFA7E93984F8D826C1293B870D832A5692B7B9FA6C55E0ABBB27FF46A1A08'

Exp mod Q:
'81BD89CE35CAC0678D8995352A41FC95BE1B3435280367780BEFFDF95772D4B510C1EA2FF0A407D10E4B23C29C4CF4EFD6EDC6F7D5BD12443B96A815519A389C3D95DB05DF18C76B'

Exp mod P:
'8CBA6045E0B281B4CBFA64E6739113DD6351E6ADDBE53747907D78437CA802725813F8860091C1B7E212918901746314949DA4FED104BF80C87C18D6BF0F85283D858D60CFEC779B'

ICC RSA Key (128 bytes)

***Modulus*:**
'A08DF5E51FE8F5B0BE6F97A30C74888D55E756B342F1BF069199C480709C75F3BAA0D44CC4E7BC9C689F5BF22937F4B542D19D7BB198745BD777E2158EE541128A158E736A884B82C521616EF06F8D267C07B1EF798AB577AAA3C6DD8937C9B2344CECAD5AB8D529BCACA7F9ECEADE85990F1E04FEAE9FA033DF691268F9F2D5'

***Public Exponent*:**
'03'

Private Exponent:
'1AC253A62FFC28F2CA67EE9B2CBE16C238FBE3C88B284A8118444B6ABD6F68FDF470236220D14A1A
116FE4A85C33FE1E35CD9A3F48441364A3E95058ED263582D36EFA8EA4EFEEA24221C54C02FB5DC3A
E17978BD6CE6B68A24B3B13C8613A2E1E0A531BA171AF7E1EFF444BFF72500389F6642F0F62E49A430C
6DF70C07EE0D'

Private Key Split for CRT:

Factor p:
'CC3826F692BDC25E315F6457DB008305F6DFB80FA61CCF4B92FD14B11F2A3CBA10FEC0C26735FEECA
2AACF09E0ADA62876C1F391BF4A16458B9D5EC73CE09C13'

Factor q:
'C9438824FA2AF15706F75D4F038AD78A709A6C98CA9761B849E34FB5B7C62FE36F1039452AD8B9486
0063F280F8F5847E686D158E3132DBD15F77680E3E9C277'

q^-1 mod p:
'B8940CF653E0D59DA5EB369242F842EDF35F370B6D719AA77CB193D246AFA0EA87D45BF26465B09A
2A37E42766E6C42C8C6174C7DD817D0610C5D92FBC2D8487'

p^-1 mod q:
'135B552FE8CEF3F1C787ABE294FCE7A5DB9598D2039E5F9A81AE5F8274418E2AA2F0D6CE9F93E36D9
177E6A8A4E9A5882BF301F16FDEEF08C813B3433C1FB637'

Exp mod p:
'88256F4F0C7E819420EA42E53CAB0203F9EA7AB519688A3261FE0DCB6A1C287C0B5480819A23FF486
C71DF5BEB1E6EC5A4814D0BD4DC0ED907BE3F2F7DEB12B7'

Exp mod q:
'862D056DFC1CA0E4AF4F938A025C8FB1A066F310870F967ADBECDFCE7A841FECF4B57B8371E5D0DA
EAAED4C55FB4E5854459E0E5ECB773D363FA4F0097F12C4F'

Appendix C: Glossary

Term	Description
M/Chip 4 Application	The M/Chip Select 4 and M/Chip Lite 4 applications as specified in the *M/Chip 4 Card Application Specifications for Credit and Debit.* When behavior is specific to one of the applications, the specific application name, i.e., M/Chip Lite 4 application or M/Chip Select 4 application, is used.
***PayPass*—M/Chip Application**	The M/Chip 4 application, extended for contactless communication as specified in the *PayPass*—M/Chip Technical Specification.
***PayPass*—M/Chip Card**	Dual interface card with the *PayPass*—M/Chip Application accessible over the contact and contactless interface.
***PayPass*—M/Chip Terminal**	A terminal accepting *PayPass*—M/Chip cards using a transaction flow similar to the EMV contact transaction flow, capable of offline card authentication and Terminal Risk Management. This terminal may also accept magnetic stripe cards and contact cards. The *PayPass*—M/Chip terminal must accept *PayPass*—Mag Stripe transactions. It may also accept other contactless schemes.
***PayPass* Technology**	The MasterCard specific implementation of ISO/IEC 14443. *PayPass* uses the technology as defined in the *PayPass*—ISO/IEC 14443 Implementation Specification for the wireless ("contactless") exchange of data between card and terminal. To achieve interoperability, MasterCard *PayPass* requires a specific implementation of the ISO/IEC 14443 standard.
***PayPass* Transaction**	A payment transaction using *PayPass* Technology for the data exchange between card and terminal.
***PayPass* Transaction Time**	The time the *PayPass* card needs to be present in the terminal's electromagnetic field to allow for a complete data exchange. The completion of the data exchange is indicated by a beep and a visual indication. Any processing done by the terminal after the card has been removed is excluded from the *PayPass* Transaction Time.

MasterCard International

© 2006
MasterCard International Incorporated